Protection des données dans le secteur de la « police » et de la « justice »

Forget, Catherine

Published in:
Société numérique et droit pénal

Publication date:
2019

Document Version
le PDF de l'éditeur

PROTECTION DES DONNÉES DANS LE SECTEUR DE LA « POLICE » ET DE LA « JUSTICE »

Catherine FORGET
Chercheuse à l'UNamur
Avocate au Barreau de Bruxelles

Introduction

Parallèlement à l'adoption du Règlement général sur la protection des données (ci-après R.G.P.D.)[1] et dans le contexte de la lutte contre le terrorisme et la grande criminalité, l'Union européenne s'est récemment dotée de la Directive 2016/680[2] (ci-après Directive 2016/680) visant à réglementer la protection des données dans le secteur de la « police » et de la « justice ». À cette fin, elle fixe une base commune de protection des données en vue de faciliter l'échange d'informations entre les autorités répressives[3] et, en ce sens, participe à la concrétisation de « l'espace de liberté, de sécurité et de justice »[4]. De manière inédite, elle encadre les traitements de données à caractère personnel des autorités compétentes, que ce traitement ait lieu sur le territoire interne des États membres ou au-delà. En effet, la décision-cadre 2008/977[5], à laquelle elle succède, avait une portée limitée en raison de la limitation

1 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (texte présentant de l'intérêt pour l'EEE), *OJ L 119*, 4 mai 2016, p. 1. Pour un commentaire, voy. K. ROSIER et C. DE TERWANGNE (dir.), *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018.

2 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *OJ L 119*, 4 mai 2016, pp. 89–131. Pour un premier commentaire, voy. P. DE HERT et V. PAPAKONSTANTINOU, *New Journal of European Criminal Law*, vol.7, Issue 1, 2016, pp. 7-19.

3 Communication de la Commission au Parlement européen, au Conseil européen et au Conseil, Quatrième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, Bruxelles, 25 janvier 2017, *COM 52017*, 41 final.

4 Considérant 2 de la directive 2016/680.

5 Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *JO L350/60*, 30 décembre 2008, pp. 60 et s. (ci-après « décision-cadre 2008/977/JAI »).

du champ d'application aux flux transfrontières de données sans être applicable aux traitements internes. Elle présente par ailleurs une certaine flexibilité, tant au niveau de la forme juridique choisie – à savoir une directive plutôt qu'un règlement – qu'au niveau du fond, cherchant à ménager un certain équilibre entre le droit à la protection des données et les intérêts liés à la sécurité au sens large. Pour le surplus, la différence entre le R.G.P.D. et la Directive 2016/680 se situe surtout au niveau des droits des personnes concernées tels que le droit à l'information, le droit d'accès, le droit d'opposition, ou encore le droit à l'oubli mais aussi par le fait qu'elle n'impose aucun système contraignant de sanctions administratives.

La Directive 2016/680 a récemment été transposée en droit belge suite à l'adoption de la loi du 30 juillet 2018 entrée en vigueur le 5 septembre 2018[6]. Cette loi implémente à la fois le R.G.P.D. (titre 1er), transpose la Directive police (titre 2) et encadre les activités de traitement par les autorités hors champ d'application de l'UE tels que les services de renseignements, la défense et l'armée (titre 3). Dans le cadre de cette contribution, après avoir fait un tour d'horizon relatif aux instruments de protection des données dans le secteur de la police et de la justice, nous présenterons les lignes de force du titre 2 de la loi du 30 juillet 2018. Par ailleurs, nous ne manquerons pas de faire référence au R.G.P.D., par exemple en cas de flux de données entre les entités privées et les autorités répressives. Nous ne chercherons pas à être exhaustif au risque de perdre le lecteur dans une matière particulièrement technique, mais ferons en sorte de mettre l'accent, à l'aide d'exemples, sur certains points susceptibles de mener à des divergences d'interprétation ou à des difficultés et ce, à la lumière des recommandations du Contrôleur européen de la protection des données (ci-après C.E.P.D.)[7] et du Groupe de travail de l'article 29 (ci-après Groupe 29) auquel a succédé, depuis le 25 mai 2018 suite à l'entrée en vigueur du R.G.P.D., le Comité européen de la protection des données[8].

6 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

7 Le C.E.P.D. se définit comme « une autorité de contrôle indépendante, qui veille à ce que les institutions et organes communautaires respectent leurs obligations en matière de protection des données. Ces règles sont énoncées dans le *règlement (CE) nº 45/2001* relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données ».

8 Le Groupe de travail de l'article 29 est un organe consultatif européen indépendant sur la protection des données. Depuis le 25 mai 2018, le Comité européen de la protection des données lui a succédé. Dans le cadre de cette contribution, nous ferons cependant référence au Groupe 29, les avis ayant été adoptés sous

I. Instruments de protection des données dans le secteur de la police et de la justice

Les traitements de données à caractère personnel dans le secteur de la police et de la justice sont encadrés par différents instruments adoptés tant par le Conseil de l'Europe que par l'Union européenne. En effet, tout traitement de données à caractère personnel par les autorités, qu'elles soient policières ou judiciaires, constitue une ingérence dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel.

Au niveau du Conseil de l'Europe, l'article 8 de la Convention européenne des droits de l'homme (ci-après C.E.D.H.)[9] garantit le droit au respect de la vie privée. Ce droit n'est cependant pas absolu. L'article 8, § 2, de la C.E.D.H. autorise une ingérence d'une autorité publique dans l'exercice de ce droit pour autant que cette ingérence soit prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. Le critère de légalité exige une réglementation « claire, prévisible et accessible » assurant une protection contre les risques d'abus et d'arbitraire[10] et permettant au justiciable, si besoin en s'entourant de conseils éclairés, de régler sa conduite[11]. Le critère de nécessité s'examine à la lumière des garanties offertes par la disposition tout en tenant compte de la marge d'appréciation laissée aux États membres[12].

Dans l'interprétation de l'article 8 de la C.E.D.H. est prise en compte la Convention 108 du Conseil de l'Europe, seul instrument contraignant de portée internationale[13] en matière de protection de données. Ce texte

l'empire de la directive 95/46/CE (Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.*, L. 281, 23 novembre 1995, p. 31).

9 Convention européenne des droits de l'homme, S.T.C.E., n° 005, 1950. Au niveau du Conseil de l'Europe, l'article 8, § 1er, garantit le droit à la vie privée. Cet article inclut, au terme d'une jurisprudence abondante, le droit à la protection des données à caractère personnel (voy. Cour E.D.H., 4 mai 2000, *Amann c. Suisse*, n° 27798/5, § 65).

10 Voy. entre autres : Cour E.D.H., *Malone c. Royaume-Uni*, 2 août 1984, série A, n° 82, § 67.

11 Voy. entre autres : Cour E.D.H., *Sanoma Uitgevers B.V. c. Pays-Bas*, 14 septembre 2010, n° 38224/03, § 81.

12 Pour une analyse des critères établis par la Cour E.D.H., voy. Division recherche de la Cour E.D.H., *Sécurité nationale et jurisprudence de la Cour européenne des droits de l'Homme*, Strasbourg, Conseil de l'Europe, 2013 et Groupe 29, Avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, 10 avril 2014.

13 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *S.T.C.E.*, n° 108, 1981.

pose les principes généraux relatifs à la protection des données, à savoir les principes de loyauté, de licéité, de finalité, de qualité et de proportionnalité tout en admettant certaines dérogations dans le cadre de la lutte contre « la répression des infractions pénales »[14]. Particulièrement importante pour notre propos, la recommandation R (87)15 vise à réglementer l'utilisation de données à caractère personnel dans le secteur de la police[15] tout en s'inspirant des principes retenus par la Convention 108. Depuis son adoption, cette recommandation a fait l'objet de plusieurs évaluations (en 1993, 1998 et 2002). En 2010, le comité consultatif de la Convention 108 a décidé de réaliser une étude sur l'utilisation de données à caractère personnel dans le secteur de la police dans l'ensemble de l'Europe. Cette évaluation a montré que ladite recommandation constituait toujours un point de départ approprié pour élaborer des réglementations en droit national[16]. Il fut alors suggéré d'émettre un instrument contraignant susceptible d'être déployé dans des secteurs jusqu'alors souvent parallèles : celui des forces de police et celui des agences de sécurité et de renseignement[17], suggestion qui n'a finalement pas été suivie.

Au sein de l'Union européenne, la Charte des droits fondamentaux (ci-après la Charte) garantit le droit à la vie privée et le droit à la protection des données à caractère personnel[18]. À la différence de l'article 8, § 1er, de la C.E.D.H., celle-ci distingue expressément les deux droits et encadre dès lors tout traitement de données à caractère personnel indépendamment d'une atteinte éventuelle à la vie

14 Art. 9 de la Convention 108. Notons que la Convention 108 fait l'objet d'un protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données. Ce texte prévoit tout d'abord l'établissement d'autorités de contrôle chargées d'assurer le respect des lois ou règlements introduits par les États en application de la Convention concernant la protection des données personnelles et les flux transfrontières de données. Ensuite, elle encadre les flux transfrontières de données vers des pays tiers, lesquelles ne pourront être transférées que si elles bénéficient, dans l'État ou l'organisation internationale destinataire, d'un niveau de protection adéquat (Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, *S.T.C.E.*, n° 181, Strasbourg, 8 novembre 2001).

15 Comité des ministres du Conseil de l'Europe, Recommandation R(87)15 du 15 septembre 1987 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (ci-après Recommandation N° R(87)15).

16 Conseil de l'Europe, rapport « Recommandation (87)15 – Vingt-cinq ans après – rapport final », Strasbourg, 18 février 2014.

17 Notons que suite à cette évaluation, le Conseil de l'Europe a élaboré un guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police fournissant des éléments d'orientation sur l'implication de ces pratiques au niveau opérationnel. (Comité consultatif de la Convention pour la protection des données des personnes à l'égard du traitement automatisé des données à caractère personnel, « Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police », Strasbourg, 15 février 2018.)

18 Art. 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

privée[19]. L'article 52, § 1er, de la Charte autorise les États membres à limiter la portée des droits et libertés par la voie législative pour autant que la mesure respecte le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elle soit nécessaire et réponde effectivement à un objectif d'intérêt général reconnu par l'Union[20]. Depuis l'entrée en vigueur du traité de Lisbonne en 2009[21], la Charte a acquis force juridique obligatoire offrant un terrain neuf à la Cour de justice de l'Union européenne s'émancipant progressivement de la jurisprudence de la Cour de Strasbourg. Elle a peu à peu développé une jurisprudence relative au droit à la protection des données[22] teintée par des décisions considérées à maints égards comme historiques[23].

Il est important de noter qu'à la différence du Conseil de l'Europe ayant pour objectif de favoriser en Europe un espace démocratique et juridique commun, organisé autour de la Convention européenne des droits de l'homme et d'autres textes de référence sur la protection de l'individu, l'Union européenne a un parcours législatif marqué entre le besoin de faciliter les flux transfrontières de données à des fins de sécurité nationale et la nécessité d'assurer le droit à la protection des données dans un domaine relevant initialement des prérogatives de la puissance publique. Dès lors, ce n'est que tardivement et peu après les attentats terroristes de Londres et de Madrid en 2004 et 2005 que l'Union européenne s'est dotée de la décision-cadre 2008/977 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Son objectif était d'améliorer la coopération entre services répressifs, en particulier en matière de prévention et de détection des infractions pénales, en respectant strictement les principes essentiels en matière de protection des données. Elle fut néanmoins fortement critiquée en raison du déséquilibre patent en faveur des impératifs de sécurité publique au détriment de la protection

19 C. DOCKSEY, « Articles 7 and 8 of the EU Charter: two distinct fundamental rights », in *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, pp. 71 et s.

20 Art. 52, § 1er, de la Charte des droits fondamentaux de l'Union européenne.

21 Art. 6, § 1er, du Traité sur l'Union européenne, *J.O.*, 2012, C 326.

22 S. PEYROU, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la C.J.U.E. », in *Protection des droits fondamentaux dans l'Union européenne*, Bruxelles, Bruylant, 2015, p. 229.

23 Voy. entre autres : C.J.U.E., 6 octobre 2015, *Schrems c. Data Protection Commissionner of Ireland*, C-362/14 ; C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 et C-594/12 ; C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB c. Post-och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson e.a.*, aff. jointes C-203/15 et C-698/15 ; C.J.U.E., 26 juillet 2017, avis 01/2015.

des droits fondamentaux[24]. De plus, son impact fut relativement limité, celle-ci excluant de son champ d'application les traitements de données réalisés sur le territoire national des États membres[25].

Dans le cadre du train de mesures législatives visant à réformer la législation de l'Union sur la protection des données, une proposition de directive applicable au secteur de la « police » et de la « justice » fut déposée en décembre 2012[26]. Après trois années de négociations, la Directive 2016/680 a été adoptée avec pour délai de transposition le 6 mai 2018[27]. Calquée sur la structure et la logique du R.G.P.D., elle fixe un corps de règles commun de protection des données adapté au domaine pénal assurant une certaine harmonisation afin de favoriser la libre circulation de ces données au sein de l'Union et dès lors, une meilleure efficacité relative à la coopération judiciaire et policière[28]. Dans l'esprit du Traité de Lisbonne[29], elle vise également à protéger les libertés et droits fondamentaux des personnes physiques et, en particulier, leur droit à la protection des données[30] tout en laissant la possibilité aux États membres de prévoir des garanties plus étendues pour les personnes concernées[31].

Au niveau national enfin, outre l'article 22 de la Constitution garantissant le droit au respect de la vie privée, la Belgique s'est récemment

24 C.E.P.D., avis du 27 avril 2007, *J.O.*, C 139, 23 juin 2007, p. 1 ; F. Dumortier, C. Gayrel, J. Jouret, D. Moreau et Y. Poullet, « La protection des données dans l'Espace européen de liberté, de sécurité et de justice », *J.D.E.*, 2010/2, n° 166, pp. 33 et s.

25 Cette ambiguïté ne manqua pas d'être relevée par le C.E.P.D. soulignant qu'il peut s'avérer délicat de déterminer à l'avance si une information est susceptible de faire l'objet d'un flux transfrontière entre les États membres. (C.E.P.D., Avis du 19 décembre 2005 sur la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, *J.O.*, C. 47, 25 février 2006).

26 Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012)0010, 25 janvier 2012.

27 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.*, L. 119, 4 mai 2016, pp. 89 et s. (ci-après directive 2016/680).

28 Considérants 7 et 25 de la Directive 2016/680 et C.E.P.D., avis n° 6/2015, une nouvelle étape vers une protection européenne complète de données, recommandations du C.E.P.D. sur la directive pour la protection des données dans les secteurs police et justice, 28 octobre 2015, p. 5 (ci-après C.E.P.D., avis n° 6/2015).

29 Le considérant 10 de la Directive 2016/680 fait référence à la déclaration n° 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, annexée au traité de Lisbonne. Au terme de celle-ci, « la conférence a reconnu que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines ».

30 Art. 1er, § 2, a, de la Directive 2016/680.

31 Art. 1er, § 3, de la Directive 2016/680.

dotée de la loi du 30 juillet 2018[32]. Comme déjà précisé ci-avant, cette loi implémente à la fois le R.G.P.D. (titre 1er), transpose la Directive police (titre 2) et encadre les activités de traitement par les autorités hors champ d'application de l'UE tels que les services de renseignements, la défense et l'armée (titre 3). Comme l'a souligné l'Autorité de la protection des données dans son avis[33], on peut regretter qu'un texte d'une telle ampleur et d'une telle importance fut adopté dans l'urgence impliquant *a fortiori* des difficultés lors des travaux parlementaires pour soumettre des observations pertinentes en temps utile[34].

II. Titre 2 de la loi du 30 juillet 2018

Section 1. *Champ d'application matériel*

À l'instar de la Directive 2016/680, le titre 2 de la loi du 30 juillet 2018 (ci-après titre 2) encadre tout « traitement de données à caractère personnel par les autorités compétentes dans le domaine de la prévention et la détection des infractions pénales, les enquêtes et poursuites en la matière ainsi que l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données »[35].

Sont donc ici visés les traitements de données à caractère personnel relatifs aux infractions pénales ainsi que leur « prévention », c'est-à-dire les données traitées dans le cadre d'une enquête spécifique, mais aussi au-delà de ce cadre, par exemple pour acquérir une meilleure compréhension de certains phénomènes[36]. Par ailleurs, même si la référence à la notion de « menace » pourrait laisser penser que la Directive 2016/680 s'applique au traitement de données relatif à la sécurité nationale intérieure, il s'agit d'un domaine dans lequel l'Europe n'est en principe pas habilitée à légiférer[37], ce domaine devrait

32 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

33 La Commission de la protection de la vie privée – qui devient avec l'entrée en application du R.G.P.D., l'Autorité de protection des données –, a regretté de devoir donner son avis sur un texte d'une telle ampleur et d'importance pour l'encadrement des données à caractère personnel dans un délai extrêmement court (C.P.V.P., avis 33/2018 relatif à l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 5).

34 *Doc. parl.*, Ch. repr., sess. ord., 2017-2018, n° 54-3126/003, p. 16.

35 Art. 1er de la Directive 2016/680 et art. 27 de la loi du 30 juillet 2018.

36 Considérant 27 de la Directive 2016/680.

37 En principe, ce domaine reste de la seule responsabilité de chaque État membre de sorte que l'UE n'est pas compétente pour légiférer en la matière (art. 4, § 2, du traité sur l'Union européenne).

donc rester hors champ d'application de la Directive 2016/680[38]. Le législateur national encadre les activités des services de renseignement dans un titre distinct, à savoir, le titre 3 de la loi du 30 juillet 2018. En revanche, conformément à la Directive 2016/680, le titre 2 inclut les traitements effectués dans le cadre de « la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »[39], c'est-à-dire les activités menées par la police ou par les autorités répressives à des fins de maintien de l'ordre public[40], entre autres lors de manifestations, de grands événements sportifs et d'émeutes[41] et ce, sans savoir au préalable si un incident constitue une infraction pénale ou non[42]. Le titre 2 inclut également dans son champ d'application les activités de police dans le cadre des règles de sanctions de droit administratif pour autant qu'elles recouvrent un caractère « pénal » au sens de la jurisprudence de la Cour de justice de l'Union européenne[43], telles qu'en principe les sanctions administratives communales[44].

38 En ce sens, le considérant 14 de la Directive 2016/680 indique exclure de son champ d'application les activités qui ne relèvent pas du droit de l'Union, telles les activités des agences ou des services responsables des questions de sécurité nationale. Cependant, ni le droit de l'UE, ni la jurisprudence de la C.J.U.E. n'offrent une définition claire de ce que revêt le terme « sécurité nationale ». Néanmoins, différents traités de l'UE y font référence, ou font référence à des notions étroitement liées, telles la sécurité intérieure, la sûreté de l'État et la défense, domaines pour lesquels l'UE est habilitée à légiférer (Groupe 29, Document de travail sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, WP228, 5 décembre 2014, p. 23.) L'exemple le plus couramment cité est celui de la lutte contre le terrorisme (voy. Directive (UE) 2017/541 relative à la lutte contre le terrorisme, *J.O.*, L 88, 31 mars 2017, p. 6). Selon le Groupe 29, pour déterminer ce qu'il y a lieu d'entendre par « sécurité nationale », il convient de tenir compte de la situation politique et des acteurs concernés sans que cette exclusion puisse servir d'excuse aux États membres pour refuser d'appliquer la législation relative à la protection des données (Groupe 29, Document de travail sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, WP228, 5 décembre 2014, p. 23.)

39 Art. 1er de la Directive 2016/680.

40 *Doc. parl.*, Ch. repr., sess. ord., 2017-2018, n° 54-3126/001, p. 68.

41 Considérant 12 de la Directive 2016/680.

42 *Ibid.*

43 Précisons que la notion d'infraction « pénale » au sens de la Directive 2016/680 est une notion autonome, interprétée à la lumière de la jurisprudence de la Cour de justice de l'Union européenne (ci-après C.J.U.E.) (considérant 13 de la Directive 2016/680) et indépendamment du droit des États membres, assurant une certaine interprétation uniforme du droit de l'Union. En effet, comme le souligne la C.J.U.E. à l'égard du respect de la règle *ne bis in idem* : « Même en l'absence d'harmonisation des législations pénales des États membres, l'application uniforme du droit de l'Union requiert, selon une jurisprudence constante, qu'une disposition ne renvoyant pas au droit de ces États reçoive une interprétation autonome et uniforme, qui doit être recherchée en tenant compte du contexte de la disposition dans laquelle elle s'insère et de l'objectif poursuivi » (C.J.U.E., 27 mai 2014, *Zoran Spasic*, C129/14 PPU, pt 79). La qualification pénale d'une infraction en droit interne n'est donc pas déterminante pour définir le champ d'application de la directive, celle-ci visant l'ensemble des infractions – qu'elle soient pénales ou administratives – donnant lieu à des sanctions recouvrant un caractère « punitif et dissuasif » (Ces critères ont notamment été retenus par la C.J.U.E. à l'égard de la reconnaissance mutuelle des sanctions pécuniaires infligées en cas d'infraction routière. Voy. C.J.U.E., 14 novembre 2013, *Baláž*, C-60/12, pt 35). La Cour E.D.H. applique le « test Engel » et prend en considération les critères suivants : la qualification de l'infraction en droit national, la nature de l'infraction et le degré de gravité de la sanction infligée. L'objectif est d'éviter qu'une personne puisse être poursuivie sans bénéficier des protections découlant d'une procédure pénale au motif d'être qualifiée de procédure administrative par le législateur par exemple (Cour E.D.H., *Engel et al. c. Pays-Bas*, 8 juin 1976, série A, n° 22).

44 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2017-2018, n° 54-3126/001, p. 69.

En outre, la Directive précitée indique que par « autorité compétente », il y a lieu d'entendre toute autorité publique compétente ainsi que, de manière large, tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins visées par la Directive[45]. Dès lors, si la gestion des prisons est confiée à une entreprise privée par exemple, les traitements de données effectués dans le cadre des finalités visées par la Directive 2016/680 devraient relever du champ d'application de la Directive 2016/680 et donc du titre 2. À l'inverse, lorsqu'une autorité compétente traite des données à caractère personnel à d'autres fins que celles visées par le titre 2, par exemple, dans le cadre de la gestion du personnel, elle devrait être soumise aux dispositions du R.G.P.D. lorsqu'elle traite de telles données[46].

Le législateur national délimite toutefois davantage le champ d'application du titre 2 que la Directive 2016/680, en énumérant exhaustivement les différentes « autorités compétentes » visées dans ce cadre. Ainsi, l'article 26, 7°, de la loi du 30 juillet 2018 indique qu'il s'agit : des services de police, des autorités judiciaires, c'est-à-dire les cours et tribunaux du droit commun et le ministère public[47] ; du Service d'enquête du Comité P dans le cadre de ses missions judiciaires[48] ; de l'Inspection générale de la police fédérale et de la police locale ; de l'Administration générale des douanes et accises, dans le cadre de sa mission relative à la recherche, la constatation et la poursuite des infractions ; de l'Unité d'information des passagers[49] ; la Cellule de traitement des informations financières ; du Service d'enquêtes du Comité R dans le

45 Art. 3, § 7, de la Directive 2016/680.

46 Art. 27 de la loi du 30 juillet 2018.

47 Plus précisément, il s'agit de l'ensemble des institutions dont la fonction est de faire appliquer la loi en tranchant des litiges tels les magistrats, les juridictions, les organes concourant à l'exercice du pouvoir de juger dans l'ordre judiciaire tels que les greffes, les collèges des cours et tribunaux et le parquet (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2017-2018, n° 54-3126/001, p. 60). En effet, à l'instar des autorités répressives, les juridictions et les autorités judiciaires sont soumises au respect des dispositions relatives au titre 2 de la loi du 30 juillet 2018, notamment lorsqu'elles traitent des données à caractère personnel dans les décisions judiciaires ou les documents relatifs aux procédures pénales. Ceci ne saurait toutefois priver les États membres de préciser les opérations et les procédures de traitement dans leurs règles de procédures pénales, telle que le Code judiciaire ou le Code d'instruction criminelle (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2017-2018, n° 54-3126/001, p. 67 et consid. 20 de la Directive 2016/680).

48 En vertu de l'article 16, alinéa 3, de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (*M.B.*, 26 juillet 1991), le Comité P est compétent pour « d'initiative ou sur réquisition du procureur du Roi, de l'auditeur militaire ou du juge d'instruction compétent, il effectue, en concurrence avec les autres officiers et agents de police judiciaire et même avec un droit de prévention sur ceux-ci, les enquêtes sur les crimes et délits mis à charge des membres des services de police et de l'Organe de coordination pour l'analyse de la menace ».

49 L'Unité d'information des passagers est un organe administratif qui reçoit, dans une première phase, des données à caractère personnel de compagnies aériennes dans le cadre de l'application du R.G.P.D., mais couple, dans une deuxième phase, les données à caractère personnel à des données policières en vue de la

cadre de ses missions judiciaires[50]. Le champ d'application du titre 2 est donc déterminé à la fois par la finalité répressive poursuivie par le responsable du traitement et par la qualité d'« autorités compétentes » telle que définie par la loi. Pour le surplus, le législateur indique que les autres autorités administratives, même si elles ont des compétences de contrôle, d'inspection ou de poursuite de certaines infractions, ne sont pas considérées comme des autorités compétentes au sens du titre 2 de la loi du 30 juillet 2018[51]. Ceci implique que, par exemple, un agent de société de transport en commun ou un agent des entreprises de gardiennage désigné par le conseil communal, constatant une infraction pouvant faire l'objet d'une sanction administrative communale[52], n'est pas soumis au champ d'application du titre 2 de la loi du 30 juillet 2018, mais au R.G.P.D.

Les travaux préparatoires justifient cette interprétation restrictive en indiquant qu'à l'instar de toute loi spéciale dérogeant au régime général institué par le R.G.P.D., elle doit être interprétée de manière stricte[53]. De plus, le législateur rappelle que la Directive 2016/680 succède à la décision-cadre 2008/977/JAI de sorte qu'il convient de veiller à ce que son champ d'application reste similaire[54]. Même si cette approche pourrait paraître aller à l'encontre de l'esprit de la Directive 2016/680, la Commission de la protection de la vie privée ne s'oppose pas à un tel régime soulignant que les activités de traitement (avec une finalité judiciaire) des instances et organes non comprises dans le titre 2 et relevant du R.G.P.D. peuvent relever de l'exception prévue par l'article 23 du R.G.P.D.[55]. Cette disposition autorise les États membres à limiter, par mesures législatives, la portée des obligations et des droits des personnes concernées quant au traitement de leurs données[56]. En consé-

prévention et la détection des infractions terroristes et des formes graves de criminalité ainsi que pour les enquêtes et les poursuites en la matière (loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017).

50 En vertu de l'article 40, alinéa 3, de la loi organique du 18 juillet 1991, le Comité R est compétent pour : « d'initiative ou sur réquisition du procureur du Roi, de l'auditeur militaire ou du juge d'instruction compétent, effectuer, en concurrence avec les autres officiers et agents de police judiciaire et même avec un droit de prévention sur ceux-ci, les enquêtes sur les crimes et délits à charge des membres des services de renseignement et de l'Organe de coordination pour l'analyse de la menace ».

51 *Doc. parl.*, Ch. repr., sess. ord., 2017-2018, n° 54-3126/001, p. 62.

52 Art. 21, § 1er, de la loi du 24 juin 2013 relative aux sanctions administratives communales, *M.B.*, 1er janvier 2014.

53 *Doc. parl.*, Ch. repr., sess. ord., 2017-2018, n° 54-3126/001, p. 67.

54 *Ibid*.

55 C.P.V.P., avis 33/2018 relatif à l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 62.

56 L'article 23, § 1er, du R.G.P.D. prévoit une possibilité de limiter sous certaines conditions la portée des droits garantis. La mesure considérée ne peut avoir pour effet de porter atteinte à l'essence des droits et libertés fondamentaux, elle doit être nécessaire et proportionnée dans une société démocratique pour garantir par exemple, la sécurité nationale, la sécurité publique, la prévention et la détection d'infractions

quence, ce mélange de genre n'apparaît, à première vue, pas forcément préjudiciable pour la personne concernée, celle-ci disposant des droits et garanties conférés par le R.G.P.D. *a priori* plus étendus que ne le prévoit la Directive 2016/680, si ce n'est que le R.G.D.P. ne prévoit pas de droit d'accès indirect tel que nous le décrivons *infra*[57].

Enfin, le traitement des données relatives aux condamnations pénales, aux infractions pénales et aux mesures de sûreté connexes n'est pas soumis au titre 2, mais est encadré de manière spécifique par le R.G.P.D.[58]. Il s'agit notamment des données traitées par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige[59], pour les nécessités de la recherche scientifique, historique ou statistique ou à des fins d'archives[60] ou encore pour les traitements relatifs à des données manifestement rendues publiques par la personne concernée, de sa propre initiative, pour une finalité ou plusieurs finalités spécifiques et si le traitement est limité à ces finalités[61].

Section 2. *Principes relatifs aux traitements de données à caractère personnel*

1. *Principes de licéité et de loyauté*

Selon l'article 33, § 1er, de la loi du 30 juillet 2018, un traitement est licite dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente dans le cadre des finalités visées par le titre 2 et s'il est fondé sur une obligation légale ou réglementaire. La base légale doit par ailleurs au minimum indiquer les catégories de données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement[62].

En vertu de la Directive 2016/680, la base juridique ne doit pas forcément être un acte législatif émanant du Parlement, mais doit être « claire, prévisible et accessible » conformément à la jurisprudence de

pénales ou encore pour permettre l'exécution des demandes de droit civil. Si l'article 23, § 1er, fait écho à l'article 52, § 1er, de la Charte des droits fondamentaux, il complète néanmoins celui-ci par une série de critères devant spécifiquement figurer dans la disposition nationale. Celle-ci doit notamment prévoir des dispositions relatives « aux finalités du traitement ou des catégories de traitement », « aux catégories de données à caractère personnel », mais aussi « aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ».

57 Voy. la section « droit des personnes concernées ».

58 Art. 10 de la loi du 30 juillet 2018 et art. 10 du R.G.P.D.

59 Art. 10, § 1er, 2°, de la loi du 30 juillet 2018.

60 Art. 10, § 1er, 4°, de la loi du 30 juillet 2018.

61 Art. 10, § 1er, 6°, de la loi du 30 juillet 2018.

62 Art. 33 de la loi du 30 juillet 3018.

la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme[63]. Rappelons toutefois que, même si les travaux parlementaires n'en font pas mention, l'article 22 de la Constitution exige une loi « formelle » votée par le Parlement et émanant du pouvoir législatif et non du pouvoir exécutif[64]. Dès lors, comme l'a rappelé la Cour constitutionnelle, « une délégation conférée au Roi n'est pas contraire au principe de légalité pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur »[65]. Sur ce point, l'article 22 de la Constitution est donc plus strict qu'imposé par la Directive 2016/680.

À juste titre, le titre 2 ne reprend pas les six bases de licéité du traitement du R.G.P.D. tels que l'intérêt légitime du responsable du traitement ou encore le consentement de la personne concernée[66]. En effet, requérir le consentement, par exemple, aurait peu de sens dans le domaine pénal ou de la justice où la personne est généralement tenue d'obtempérer au traitement de ses données et ne dispose donc pas d'une véritable liberté de choix[67]. En revanche, son consentement peut être requis en tant que garantie supplémentaire, en cas de traitement de données particulièrement sensibles par exemple[68]. Il pourra également être requis en vue de permettre un dispositif de surveillance électronique par le biais d'une géolocalisation dans le cadre de l'exécution de sanctions pénales ou encore pour pouvoir effectuer un test ADN dans le cadre d'une enquête[69], comme le prévoit par exemple les articles 44*ter* et suivant du Code d'instruction criminelle. En ce cas, la personne doit être informée

63 Considérant 35 de la Directive 2016/680. Pour la jurisprudence de la Cour E.D.H. voy. notamment : Cour E.D.H., *Malone c. Royaume-Uni*, 2 août 1984, série A, n° 82, § 67 ; C.J.U.E., 17 décembre 2015, *WebMindLicenses*, C-419/14, § 81.

64 P. De Hert, « Le droit fondamental à la vie privée et le droit fondamental à la protection des données à caractère personnel », *Manuel sur la vie privée et la protection des données* (P. De Hert éd.), Bruxelles, Politéia, feuillets mobiles, mise à jour n° 9 (2002), également disponible à l'URL : http://www.vub.ac.be/LSTS.

65 C. const., n° 135/2004, 22 juillet 2004.

66 Art. 6 du R.G.P.D.

67 Considérant 35 de la Directive 2016/680. Cette approche rejoint celle du R.G.P.D. selon laquelle le consentement ne peut être donné librement et constituer une base juridique valable pour le traitement de données à caractère personnel « lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière ». Considérant 43 du R.G.P.D.

68 Selon le considérant 37 de la Directive 2016/680, le traitement des données sensibles exige le respect des garanties appropriées pour les droits et libertés de la personne concernée, mais aussi le traitement de ces données devrait être autorisé par la loi « lorsque la personne concernée a expressément marqué son accord au traitement qui est particulièrement intrusif pour elle. Toutefois, l'accord de la personne concernée ne devrait pas constituer en soi une base juridique pour le traitement de ces données à caractère personnel sensibles par les autorités compétentes ».

69 Considérant 35 de la Directive 2016/680.

de manière claire et non ambiguë de la possibilité de retirer son consentement à tout moment [70]. Précisons qu'à défaut de consentement, l'enquêteur devra obtenir l'autorisation d'un juge d'instruction pour procéder à l'analyse de l'ADN d'une personne conformément à l'article 90*undecies* du Code d'instruction criminelle.

2. *Principe de finalité*

Le principe de finalité, pierre angulaire du régime de la protection des données [71], permet de concrétiser celui de la minimisation des données : il s'agit premièrement de comprendre pourquoi des données sont traitées avant de pouvoir déterminer celles qui doivent l'être afin d'éviter le risque d'en traiter davantage que nécessaire pour atteindre l'objectif poursuivi [72]. À l'instar des règles prévues par le R.G.P.D., les données traitées par les autorités compétentes doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent être traitées d'une manière incompatible avec ces finalités [73].

Le traitement ultérieur de ces données, par le même ou par un autre responsable du traitement, pour l'une des finalités visées par le titre 2, est autorisé pour autant qu'il soit encadré par une base légale et qu'il soit nécessaire et proportionné au regard de cette autre finalité [74]. Ainsi, le ministère public traitant certaines données à caractère personnel dans le cadre d'une enquête pourrait réutiliser ces données après la condamnation de la personne concernée dans le cadre de l'exécution des peines pour autant que cela soit prévu par la loi. En revanche, le traitement ultérieur à d'autres fins que celles visées par le titre 2 de la loi du 30 juillet 2018 n'est pas permis à moins d'être autorisé par une loi, un décret, une ordonnance, le droit de l'Union européenne ou un accord international [75]. Dès lors, par exemple, le ministère public est tenu de communiquer au fonctionnaire chargé de l'établissement ou du recouvrement d'impôt, tous renseignements ainsi que tous actes, pièces, registres et documents quelconques qu'il détient afin de lui permettre d'assurer l'établissement

70 Groupe 29, Opinion on some key issues of the Law Enforcement (EU 2016/680), WP258, 29 novembre 2017, p. 9 (ci-après Groupe 29, avis 2017).
71 Groupe 29, opinion 03/2013 on purpose limitation, 3 avril 2013.
72 Groupe 29, avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, 27 février 2014, pt 5.7. Voy. égal. C.E.P.D., Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, 11 avril 2017.
73 Art. 28, 2°, de la loi du 30 juillet 2018.
74 Art. 29, § 1er, de la loi du 30 juillet 2018.
75 Art. 29, § 2, de la loi du 30 juillet 2018.

ou la perception des impôts établis par l'État[76]. Si ces informations font l'objet d'une procédure judiciaire, l'autorisation expresse du procureur fédéral ou du procureur général est néanmoins requise[77].

Compte tenu de l'importance du principe de finalité, le C.E.P.D. recommandait néanmoins « d'ajouter des éléments supplémentaires au texte afin de délimiter la notion de limitation de la finalité dans le domaine de la police et de la justice et de préciser la notion de traitement ultérieur incompatible »[78]. Il soulignait le danger d'un traitement ultérieur ayant une finalité totalement différente et prenait pour exemple le risque, par ailleurs souvent dénoncé[79], que des données collectées à des fins policières puissent être traitées ultérieurement à des fins d'immigration[80]. Un autre exemple interpellant est celui des flux de données de plus en plus récurrents entre services de renseignement et services de police lesquels poursuivent pourtant des missions différentes[81]. Dès lors, afin de garantir l'effectivité du principe de finalité, le Groupe 29 recommande d'examiner la compatibilité du traitement ultérieur en tenant compte des critères suivants : le lien pouvant exister entre les deux finalités ; le contexte initial dans lequel les données ont été collectées et les attentes raisonnables de la personne concernée quant à ce traitement ultérieur ; la nature des données à caractère personnel et les conséquences possibles du traitement ultérieur envisagé pour les droits des personnes concernées ; et les garanties offertes par le responsable du traitement pour assurer un traitement loyal et licite des données[82].

3. *Principe d'exactitude*

De manière analogue aux dispositions prévues par le R.G.P.D., les données à caractère personnel traitées dans le cadre des finalités visées par le titre 2 doivent être exactes et, si nécessaire, mises à jour

76 Art. 327, § 1er, du Code des impôts sur les revenus du 10 avril 1992, *M.B.*, 1er janvier 1992.
77 Art. 327, § 2, du Code des impôts sur les revenus du 10 avril 1992, *M.B.*, 1er janvier 1992.
78 C.E.P.D., avis n° 6/2015, p. 7.
79 Le « mix » des finalités « répressives » et de « gestion des frontières » a déjà été critiqué à de nombreuses reprises par le passé dans le cadre des discussions relatives au VIS, SIS et EURODAC. Voy., par exemple, C.E.P.D., avis sur la proposition modifiée de règlement du Parlement européen et du Conseil relatif à la création du système « EURODAC » pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE), 5 septembre 2012, p. 7.
80 C.E.P.D., avis n° 6/2015, p. 7.
81 Ce mélange de finalités est illustré dans le domaine des surveillances des communications électroniques par le Groupe 29 relevant qu'il « conviendrait de déterminer dans quelle mesure une ingérence fondée sur la sécurité nationale demeure le reflet de la réalité, maintenant qu'il apparaît que le travail des services de renseignement est plus que jamais interconnecté avec celui des autorités répressives et qu'il poursuit plusieurs objectifs différents ». Voy. Groupe 29, avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, 10 avril 2014, p. 16.
82 Groupe 29, Opinion 03/2013 on purpose limitation, 2 avril 2013, pp. 23 et s.

en prenant des mesures raisonnables pour que les données inexactes ou incomplètes soient effacées ou rectifiées « sans tarder »[83]. Par ailleurs, dans la lignée de la recommandation R (87)15, les données « fondées sur des faits » doivent, dans la mesure du possible[84], être distinguées de « celles fondées sur des appréciations personnelles »[85]. À cette fin, le responsable du traitement peut prévoir des catégories en fonction du degré d'exactitude ou de fiabilité des informations qu'il traite[86]. Le législateur national impose par ailleurs aux autorités compétentes de vérifier l'exactitude des données avant leur transmission ou mise à disposition[87] et de fournir au destinataire des données des informations nécessaires lui permettant de s'assurer de l'exactitude des données et de leur niveau de mise à jour[88].

Concernant la Banque de données nationale générale (ci-après B.N.G.)[89], par exemple, le Comité P a révélé dans un rapport de 2003 que l'information était parfois traitée un peu à la légère. En effet, dans un dossier, il était indiqué qu'une personne qui aurait été porteuse du virus du sida aurait eu l'intention de contaminer les fonctionnaires de police lors d'une intervention policière. Or, d'après l'enquête menée par le Comité Permanent P et par l'Organe de contrôle, l'information enregistrée reposait uniquement sur des rumeurs verbales, sans justification judiciaire ou administrative et sans évaluation approfondie[90].

4. *Durée de conservation des données*

Les données ne peuvent être conservées « sous une forme permettant l'identification des personnes concernées » pour une durée supérieure à celle nécessaire au regard de l'objectif poursuivi[91]. Ce critère a été rappelé à plusieurs reprises par la C.J.U.E. considérant que la période de conservation des données devait « toujours répondre à des critères

83 Art. 28, 4°, de la loi du 30 juillet 2018 et art. 5, d, du R.G.P.D.

84 Il s'agit d'une obligation de moyen, la fiabilité ou l'exactitude de certaines données pouvant dépendre de l'évolution d'une enquête, par exemple, les témoignages, l'appréciation des pièces d'un dossier, le statut de victime ou de témoin.

85 Art. 32, § 1er, de la loi du 30 juillet 2018.

86 Considérant 30 de la Directive 2016/680.

87 Art. 32, § 2, 1°, de la loi du 30 juillet 2018.

88 Art. 32, § 2, 2°, de la loi du 30 juillet 2018.

89 La B.N.G. est la banque de données policière qui contient les données traitées à des fins de police administrative et judiciaire et les informations dont l'ensemble des services de police ont besoin pour exercer leurs missions. Voy. art. 44/5 et s. de la loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992.

90 Comité P, rapport annuel 2003, pt 67, disponible sur : http://www.comitep.be/2003/Fr/2003FR.htm.

91 Art. 4, e, de la Directive 2016/680.

objectifs, établissant un rapport entre les données à caractère personnel à conserver et l'objectif poursuivi »[92].

Conformément à la Directive 2016/680, le titre 2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel impose de déterminer par base légale la durée maximale de conservation à l'échéance de laquelle les données sont effacées[93] et/ou d'organiser à l'échéance d'un premier délai de conservation, un examen périodique portant sur la nécessité de conserver les données compte tenu de l'objectif poursuivi[94]. Dans ce cas, la loi, le décret ou l'ordonnance doit prévoir un délai maximum de conservation[95]. Ainsi, si les données sont traitées à des fins préventives par exemple, un examen périodique pourrait permettre de vérifier si le stockage des données est toujours nécessaire d'autant qu'à la différence des données traitées dans le cadre d'une enquête pénale, aucune décision définitive n'impliquera la suppression automatique des données collectées[96]. En outre, le Groupe 29 recommande de lire l'article 5 de la Directive 2016/680 en combinaison avec l'article 6 de celle-ci et de prévoir un régime graduel du stockage des données en fonction des catégories de personnes concernées, telles les victimes, témoins, suspects ou tiers, mais aussi de prévoir des garanties supplémentaires au fil et à mesure du temps, par exemple, en renforçant les conditions d'accès aux données en fonction de l'objectif poursuivi[97].

À titre illustratif, l'article 44/9 de la loi sur la fonction de police fixe la durée de conservation des données traitées dans la Banque de données nationale générale en fonction des différentes catégories de personnes[98] et de la gravité des faits et ce, tant en matière de police administrative que de police judiciaire. Ces données doivent être archivées lorsqu'elles

92 C.J.U.E., 6 octobre 2015, *Schrems c. Data Protection Commissionner of Ireland*, C-362/14, § 93 ; C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB c. Post-och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson e.a.*, aff. jointes C-203/15 et C-698/15, § 110.

93 Art. 30, 1°, de la loi du 30 juillet 2018. À titre illustratif, la Cour européenne des droits de l'homme a considéré que la conservation de données à caractère personnel relatives à des faits ayant été classés sans suite pendant une durée de vingt ans entraînait une ingérence disproportionnée dans le droit au respect de la vie privée. Cour E.D.H., *Brunet c. France*, 18 septembre 2014, n° 21010/10.

94 Art. 30, 2°, de la loi du 30 juillet 2018.

95 Art. 30, 3°, de la loi du 30 juillet 2018.

96 Groupe 29, avis 2017, p. 4.

97 Groupe 29, avis 2017, p. 5.

98 À titre illustratif, les données traitées dans la B.N.G. à des fins de police administrative relatives au contact des représentants des associations, communiquées volontairement par celles-ci ou disponibles publiquement pour permettre la gestion des événements sont conservées durant une période de trois ans tandis que les données relatives aux personnes impliquées dans les phénomènes de police administrative sont conservées pendant une période de cinq ans (art. 44/9, § 1er, al. 1-2, de la loi sur la fonction de police). En revanche, les données traitées dans la B.N.G. à des fins de police judiciaire sont conservées durant un an, dix ans ou trente ans selon qu'il s'agit d'une contravention, délit ou crime que la personne soit suspecte, auteure ou condamnée (art. 44/9, § 2, a), al. 1-2, de la loi sur la fonction de police).

sont devenues non adéquates, non pertinentes ou excessives et doivent être effacées à l'issue d'un délai de trente ans[99]. *A contrario* de ce que suggère la Directive 2016/680, aucun examen périodique n'est prévu afin de vérifier la nécessité de conserver les données en fonction de l'objectif poursuivi. En outre, en dépit d'un délai particulièrement long, la Cour constitutionnelle a estimé qu'il n'était pas dénué de justification raisonnable de ne pas effacer immédiatement les données considérant, d'une part, qu'après archivage, les données ne peuvent être consultées que dans des situations exceptionnelles, telle que l'enquête sur les tueurs du Brabant wallon[100] et, d'autre part, que le traitement poursuit une autre finalité relevant de la loi relative aux archives[101]. Certes, durant la période « d'archivage », les données sont légalement consultables à des fins plus limitatives, il reste néanmoins que la personne concernée est en droit de se demander si cette période de rétention n'est pas contraire au prescrit selon lequel les données doivent être conservées « pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées ». Sur la base de cette logique, la Cour européenne des droits de l'homme n'a d'ailleurs pas hésité à condamner l'État français alors qu'il prévoyait un délai de conservation de vingt ans, délai inférieur à celui prévu par la loi belge[102].

Section 3. *Catégories de personnes concernées*

Conformément à la recommandation R (87)15 et à la Directive 2016/680, le titre 2 de la loi du 30 juillet 2018 impose au responsable du traitement d'établir des catégories de données en fonction des personnes concernées[103]. Doivent donc être distinguées, les données des personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale, les personnes reconnues coupables d'une infraction pénale, les victimes ou les personnes dont les faits portent à croire qu'elles pourraient être victimes d'une infraction pénale et les tiers à une infraction pénale tels que les témoins ou les personnes susceptibles de pouvoir fournir des informations aux enquêteurs[104].

99 Art. 44/10, § 1er, al. 2, de la loi sur la fonction de police.
100 *Doc. parl.*, Ch. repr., sess. ord., 2013-2014, n° 53-3105/001, p. 4849.
101 C. const., n° 108/2016, 14 juillet 2016, B.113.1.
102 Cour E.D.H., *Brunet c. France*, 18 septembre 2014, n° 21010/10.
103 Art. 31 de la loi du 30 juillet 2018.
104 *Ibid.*

À l'instar de la Directive 2016/680, le titre 2 ne prévoit pas de dispositions spécifiques relatives aux tiers autres que les témoins ou les personnes susceptibles de pouvoir fournir des informations aux enquêteurs. Pourtant, selon le Groupe 29, le traitement de leurs données « ne devrait être autorisé que dans certaines conditions spécifiques et pour autant qu'il soit absolument nécessaire à une finalité légitime, clairement définie et particulière » mais aussi « être limité à une période déterminée et l'utilisation ultérieure de ces données à d'autres fins devrait être interdite »[105]. De manière plus générale, le Groupe 29 préconise l'adoption de garanties supplémentaires à l'égard de la catégorie des personnes « non suspectes » compte tenu de l'évolution des techniques et des méthodes répressives[106].

À titre illustratif, le système « PNR » pour « *Passenger Name Record* » implique le traitement de données de personnes « non suspectes » d'avoir commis une infraction pénale[107]. Cette mesure, insérée par la loi du 25 décembre 2016[108] – adoptée dans la foulée d'une Directive européenne[109] –, impose aux transporteurs et opérateurs de voyage des différents secteurs de transport international (aérien, ferroviaire, routier et maritime) de transmettre les informations relatives à leurs passagers[110] à une banque de données gérée par le Service public fédéral Intérieur[111]. Ces données ont vocation à être analysées avant l'arrivée, le transit ou le départ d'une personne sur le territoire national[112] par l'Unité d'informations des passagers (UIP) créée au sein du SPF Intérieur[113]. Cette

105 Groupe 29, avis 01/2013, apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale, p. 3.

106 *Ibid.*

107 C.J.U.E., 26 juillet 2017, avis 01/2015. Pour une brève analyse, voy. C. FORGET, « L'avis de la C.J.U.E. sur l'accord PNR UE-Canada : une occasion ratée de réaffirmer le principe de finalité ? », *J.D.E.*, 2018, n° 247 pp. 87 et s.

108 Loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017.

109 Directive (UE) 2016/681 du Parlement européen et du Conseil, du 27 avril 2016, relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *J.O.*, L 119, 2016, p. 132. Soulignons qu'avant l'adoption de cette directive, l'Union européenne a conclu en parallèle des accords bilatéraux avec des pays tiers dont les États-Unis, le Mexique et le Canada.

110 L'article 9 de la loi PNR distingue les données API à savoir les données d'enregistrement et d'embarquement, des données PNR à savoir les données de réservation. Les données API sont des données authentiques, par exemple, données biographiques figurant sur une carte d'identité. Les données PNR comprennent davantage d'informations. Il s'agit notamment de l'itinéraire complet pour le passager, l'agence de voyage, le numéro de siège, les informations relatives aux bagages, les données d'enregistrement et d'embarquement (type de document de voyage, numéro du document, nationalité, nombre, poids et identification des bagages, numéro de transport, etc.), les modes de paiement et l'adresse de facturation, etc.

111 Art. 3 de la loi PNR.

112 Art. 15 de la loi PNR.

113 Art. 24 de la loi PNR.

méthode appliquée à des fins de « *pre-screening* »[114] permettrait de « faire émerger des profils de passagers à risque qui ne sont pas nécessairement connus ou mentionnés dans les banques de données des services »[115].

La loi du 25 décembre 2016 instituant le système PNR a fait couler peu d'encre au niveau national – outre un recours pendant à la Cour constitutionnelle introduit par la Ligue des droits de l'homme[116]. En revanche, la Directive européenne dont elle est le fruit fut fortement critiquée au niveau européen tant par le Groupe 29[117] que par le C.E.P.D.[118]. Ces derniers invoquèrent notamment son manque de proportionnalité compte tenu de son caractère systématique et massif, celle-ci s'appliquant de manière générale et indifférenciée à l'égard des passagers. De même, selon le Conseil de l'Europe, un tel mécanisme ciblant des personnes « qui n'ont commis aucune infraction » ne pourrait en aucun cas viser « un but légitime » au sens de la Charte des droits fondamentaux et de la Convention européenne des droits de l'homme d'autant qu'il existe un risque d'erreur inévitable susceptible et ainsi de mener à du profilage discriminatoire[119]. Dans le cadre de l'examen de l'accord PNR conclu entre le Conseil de l'Union et le Canada[120], la C.J.U.E. a néanmoins validé cet outil de « renseignement en matière criminelle »[121] s'appliquant à des

114 Le « *pre-screening* » consiste en « l'évaluation du risque représenté par les passagers » et s'effectue par le biais d'une corrélation entre les banques de données des services compétents ou par le biais de critères préétablis par l'UIP.

115 Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-2069/001, p. 29. En outre, les services compétents, à savoir, les services de police, la Sûreté de l'État, le Service général de renseignement et de sécurité, de services d'enquêtes liées aux infractions douanes et accises (art. 14, § 1er, 2°, de la loi PNR), ont la possibilité de procéder à des recherches ponctuelles dans les limites de leurs missions et des finalités prévues par la loi, à savoir notamment la lutte contre le terrorisme, la recherche et la poursuite de certaines infractions et la lutte contre l'immigration illégale (art. 8 de la loi PNR).

116 Recours en annulation totale ou partielle de la loi du 25 décembre 2016 relative au traitement des données des passagers, introduit par l'ASBL « Ligue des droits de l'homme ».

117 Voy. notamment : Groupe Article 29, avis 7/2010 sur la communication de la Commission relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, 12 novembre 2010 ; Groupe Article 29, avis 10/2011 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, 5 avril 2011.

118 C.E.P.D., avis n° 5/2015, Deuxième avis sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, 24 septembre 2015, pp. 4 et s.

119 Rapport du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé du Conseil de l'Europe, *Passenger Name Records, data mining & data protection: the need for strong safeguards*, 15 juin 2015, T-PD(2015)11.

120 Le 23 juin 2014, le Canada et le Conseil de l'UE signaient un accord concernant le transfert des données PNR. Le texte fut soumis pour approbation au Parlement en juillet 2014 lequel saisit la C.J.U.E. pour une demande d'avis (C.J.U.E., 26 juillet 2017, avis 01/2015).

121 Lors des négociations intra-européennes au sujet de la directive PNR, il y fut rappelé que même si les données des passagers sont liées aux déplacements, il s'agirait essentiellement d'un outil de « renseignement en matière criminelle », plutôt que d'un « instrument de contrôle aux frontières ». Voy. Proposition de

tiers non suspectés d'avoir commis une infraction, sous réserve de règles matérielles et procédurales strictes[122].

Section 4. *Catégories particulières de données*

Les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique[123], celles concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique sont qualifiées de données « sensibles »[124]. Compte tenu des risques pour les droits et libertés des personnes physiques et du danger de créer des situations discriminatoires, le R.G.P.D. interdit le traitement de ces données, sauf exceptions[125]. La Directive 2016/680, par contre, autorise le traitement de ces données sous réserve de certaines conditions[126] et ce, en dépit de l'avis du C.E.P.D.[127] et de la recommandation R (87)15[128].

Ainsi, l'article 34, § 1er, de la loi du 30 juillet 2018 autorise le traitement de données sensibles en cas de « nécessité absolue »[129] pour

directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (COM/2011/0032 final).

122 La Cour après avoir exclu le traitement des données sensibles, rappelle la nécessité de clarifier les catégories de données, de faire usage de modèles et critères « spécifiques et fiables » et « non discriminatoires » et de faire référence à des bases de données en lien avec l'objectif poursuivi. Puis, s'appuyant sur sa propre jurisprudence, la Cour rappelle que la période conservation des données devrait « toujours répondre à des critères objectifs, établissant un rapport entre les données à caractère personnel à conserver et l'objectif poursuivi ». Partant, le stockage pendant cinq ans après le départ des passagers du territoire canadien pour lesquels aucun risque n'a été identifié, ne semble présenter aucun lien « ne serait-ce qu'indirect » entre les données conservées et l'objectif poursuivi. De même, l'accès aux données devrait répondre à certaines conditions matérielles et procédurales basées sur des critères objectifs et être subordonné à un contrôle préalable par une juridiction ou une entité administrative indépendante sur demande motivée des autorités compétentes. En outre, les personnes concernées devraient bénéficier d'un droit à l'information individuelle. Par ailleurs, la communication des données PNR à un pays tiers ne devrait être admise qu'à la condition qu'il existe soit un accord entre l'Union et ce pays tiers équivalent à l'accord envisagé, soit une décision d'adéquation de la Commission. Enfin, le contrôle du respect des règles précisées par l'accord devrait être assuré par une autorité de contrôle indépendante (C.J.U.E., 26 juillet 2017, avis 01/2015, consid. 158, 165, 172, 191, 199-202, 205, 208, 214, 220, 230).

123 Les données génétiques et biométriques telles que les empreintes digitales et l'ADN, aux fins d'identifier une personne physique, sont désormais expressément définies et qualifiées de données sensibles. À ce propos voy. C. Jasserand, « Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data », *E.D.P.L*, 2016/3, pp. 297 et s.

124 Art. 34, § 1er, de la loi du 30 juillet 2018.

125 Art. 9 du R.G.P.D.

126 Art. 10 de la Directive 2016/680.

127 C.E.P.D., avis n° 6/2015, p. 7.

128 Principe 2 de la Recommandation R(87)15.

129 Dans l'avis du Groupe 29, il est fait référence à l'expression « strictement nécessaire » et non à la « nécessité absolue » et ce, conformément à la jurisprudence de la C.J.U.E. dans le cadre des arrêts récents relatifs à la protection des données (voy. entre autres : C.J.U.E., 6 octobre 2015, *Schrems c. Data Protection Commissionner of Ireland*, C-362/14 ; C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael*

autant que ce traitement soit assorti de garanties appropriées et qu'il soit autorisé par la loi, le décret, l'ordonnance, le droit de l'Union européenne ou l'accord international[130]. Pour le surplus, l'autorité compétente ou le responsable de traitement est tenu d'établir une liste des catégories de personnes ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées[131]. Le législateur n'impose donc pas expressément le respect des garanties prévues par le considérant 37 de la Directive 2016/680, à savoir : limiter la collecte des données à celles en rapport avec la personne concernée, une sécurisation adéquate des données collectées, des conditions d'accès plus strictes et l'interdiction de transmettre ces données. Dans le domaine pénal, le traitement de données sensibles est particulièrement courant. En effet, la législation sur les sanctions administratives communales, par exemple, implique le traitement de données sensibles, à savoir des données judiciaires et précise quels sont les agents susceptibles de pouvoir procéder à la constatation des infractions[132].

En outre, le titre 2 de la loi du 30 juillet 2018 reprend les deux exceptions prévues par la Directive 2016/680, à savoir qu'elle autorise le traitement de données sensibles dans le cas où les intérêts vitaux d'une personne sont en jeu[133] ou lorsque les données sont manifestement rendues publiques par la personne concernée[134]. Il faut toutefois que son intention de rendre ces informations publiques soit claire[135], par exemple parce qu'elles sont publiées dans une biographie, dans la presse ou sur un site *web*. Selon le Groupe 29, en cas de doute, cette dérogation doit être interprétée de manière restrictive puisque l'inscription à un réseau social, par exemple, pourrait inclure l'acceptation de règles de confidentialité conférant un accès tant aux fournisseurs de

Seitlinger e.a., C-293/12 et C-594/12 ; C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB c. Post-och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson e.a.*, aff. jointes C-203/15 et C-698/15). On peut toutefois raisonnablement considérer que ces termes sont équivalents. Selon le Groupe 29, l'utilisation de ces termes vise à mettre l'accent sur le respect du principe de nécessité en raison du traitement de catégories particulières de données mais aussi sur l'importance de prévoir des justifications solides pour le traitement de telles données (Groupe 29, avis 2017, p. 9.).

130 Art. 34, § 1er, 1°, de la loi du 30 juillet 2018.

131 Art. 34, § 2, de la loi du 30 juillet 2018.

132 Art. 20 et 21 de la loi du 24 juin 2013 relative aux sanctions administratives communales, *M.B.*, 1er janvier 2014. Voy. égal. : C.P.V.P., Recommandation n° 04/2010 du 19 mai 2010 d'initiative concernant la législation relative aux sanctions administratives communales et la protection des données à caractère personnel (SE-2009-042).

133 Art. 34, § 1er, 2°, de la loi du 30 juillet 2018.

134 Art. 34, § 1er, 3°, de la loi du 30 juillet 2018.

135 Groupe 29, avis 2017, p. 10.

services qu'aux autorités policières, sans que l'utilisateur en soit toujours pleinement conscient[136].

Précisons à ce propos que les sites internet accessibles *via* des moteurs de recherche tels *Google* ou *Bing* sont qualifiés de « sources ouvertes » dans la mesure où tout le monde peut y avoir accès, que cet accès soit gratuit ou payant. Selon la Convention de Budapest[137], ces pages *web* sont consultables par les enquêteurs comme par le public quelle que soit la localisation de ces données[138]. Par ailleurs, la Cour de cassation s'est récemment prononcée sur la possibilité pour les services de police de collecter des preuves sur une place de marché en ligne hébergée sur le *darknet*[139], place où s'échangeaient notamment des drogues illicites et où les utilisateurs pouvaient publier des commentaires à l'intention des autres usagers[140]. Selon le demandeur en cassation, le forum devait être considéré comme un « lieu privé » ou un « club virtuel » accessible à un nombre limité de personnes compte tenu des modalités d'inscription[141]. La Cour de cassation rejeta l'argument et considéra que cette place de marché en ligne ne pouvait être qualifiée « d'espace non accessible au public » compte tenu des modalités purement formelles pour y pénétrer. Elle rappela que, conformément à l'article 26 de la loi sur la fonction de police, les officiers de police judiciaire peuvent consulter les données publiées sur un site internet, un forum ou un blog « accessible au public »[142], c'est-à-dire « sans contrôle réel ou sans vérification sur la qualité des personnes »[143] en vue de rechercher les crimes, les délits et

136 *Ibid*.

137 Cette Convention offre aux États parties un cadre contraignant en matière de procédure pénale (Convention sur la cybercriminalité, Budapest, 23 novembre 2001, *S.T.C.E.*, n° 185). Elle a été ratifiée par la Belgique en 2012 (voy. *Loi du 3 août 2012* portant assentiment à la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, *M.B.*, 21 novembre 2012).

138 Art. 32, a), de la Convention sur la cybercriminalité, Budapest, 23 novembre 2001, *S.T.C.E.*, n° 185 ; voy. égal. art. 25, § 4, de la Décision du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol), *O.J. L. 121*, 15 mai 2009, pp. 37 et s.

139 Un réseau de type « *darknet* » permet en théorie de rester anonyme puisqu'il n'implique pas un partage public des adresses IP.

140 Cass., 28 mars 2017, R.G. n° P.16.1245.N/4.

141 Pour pouvoir pénétrer sur cette place de marché, les officiers de police judiciaire s'étaient enregistrés en faisant usage du navigateur *Tor Browser*, navigateur permettant de surfer sur le réseau *Tor* de manière anonyme, et ainsi se connecter sur le *darknet*. Pour obtenir l'adresse du site, ils avaient reçu un lien d'invitation d'un membre de la communauté généré automatiquement. Une fois connectés sur les lieux, ils procédèrent à des constatations relatives au profil et aux commentaires du suspect.

142 Cette disposition permet en effet aux officiers de police judiciaire de pénétrer, autrement dit *accéder physiquement*, dans les lieux qui leur sont légalement accessibles, à savoir, *les lieux accessibles au public, les immeubles abandonnés et les établissements hôteliers ou autres établissements de logement*. Cette base légale avait déjà été suggérée par la doctrine (à ce propos, voy. J. Kerchofs et P. Van Linthout, « Cybercrime », *Politeia*, 2013, ainsi que C. Conings et P. Van Linthout, « Sociale media – Een nieuwe uitdaging voor politie en justitie », *Panopticon*, 2012, vol. 3).

143 Selon la Cour de cassation, les utilisateurs ne pouvaient « s'attendre raisonnablement » à ce que cet espace soit limité à un cercle privé indépendamment de l'anonymat recherché par les utilisateurs par le biais de l'utilisation du navigateur *Tor Browser*. De plus, les enquêteurs n'avaient pas adopté une identité fictive crédible ou utilisé un alias provocant ou encore, fait usage d'un mot de passe, d'un *login* ou de clés de chiffrement afin de « craquer » l'accès au système informatique.

les contraventions, d'en rassembler les preuves et d'en livrer les auteurs aux tribunaux chargés de les punir[144]. Même si le caractère accessible du lieu *online* n'était pas contestable, on peut regretter qu'en l'absence de critères prévus par la loi, la Cour de cassation n'ait pas été plus stricte pour qualifier celui-ci[145]. En effet, comme l'indiquait la Commission de la protection de la vie privée, par conditions d'accès « purement formelles », il y a lieu d'entendre : « sans contrôle de l'exactitude des données et sans que cela n'empêche n'importe qui d'avoir accès »[146], et non pas un contrôle « de contenu et de qualité personnel » comme l'a pointé la Cour de cassation. En définitive, le caractère accessible ou non d'un lieu en ligne de même que le fait de rendre une information publique, est une question de fait, qui au besoin pourra être soumise à l'appréciation du juge du fond.

Section 5. *Droits des personnes concernées*

Afin de garantir l'effectivité des droits des personnes concernées, similairement au R.G.P.D., la personne concernée doit obtenir du responsable du traitement des informations relatives au traitement de manière accessible, en termes clairs, simples et faciles à comprendre et ce, par tout moyen approprié, y compris par voie électronique[147].

Plus précisément, le responsable du traitement est tenu de fournir à la personne concernée les informations suivantes : l'identité du responsable du traitement, le cas échéant, les coordonnées du délégué à la protection des données ; l'existence d'un traitement ; les finalités du traitement ; le droit d'introduire une plainte auprès de l'autorité de contrôle et les coordonnées de ladite autorité ; l'existence du droit d'accès, de rectification, d'effacement, de la limitation du traitement ; la base juridique du traitement ; la durée de conservation des données à caractère personnel ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée ; et, le cas échéant, les catégories de destinataires des données à caractère personnel[148].

144 Art. 8 du Code d'instruction criminelle.
145 Dans le même sens, voy. C. CONINGS, "De politie op het darknet", *T. Strafr.*, 2017/5, p. 331.
146 C.P.V.P., avis n° 13/2015 du 13 mai 2015 sur l'avant-projet de loi portant dispositions diverses – modifications de la loi portant création d'un organe de recours en matière d'habilitations de sécurité, de la loi sur la fonction de police et de la loi du 18 mars 2014 relative à la gestion de l'information policière (CO-A-2015-019), pt 27.
147 Art. 36 de la loi du 30 juillet 2018 et art. 12, § 1er, du R.G.P.D.
148 Art. 37, § 1er, 1° à 8°, de la loi du 30 juillet 2018.

Par ailleurs, pour assurer un traitement loyal des données, en particulier lorsque les données sont collectées à l'insu de la personne concernée[149], par des moyens secrets ou non, des informations complémentaires doivent être fournies à la personne concernée. Selon les travaux préparatoires et conformément au considérant 42 de la Directive 2016/680, ces informations peuvent figurer sur le site internet de l'autorité compétente de sorte qu'il ne s'agit pas d'une obligation de notification individuelle[150]. On peut néanmoins regretter que cette obligation d'informations complémentaires ne soit pas directement adressée à la personne concernée. En effet, à titre illustratif, dans le cadre d'un avis relatif à la loi sur les sanctions administratives communales, la Commission de la protection de la vie privée recommandait de fournir des informations complémentaires à la personne concernée « dès l'enregistrement des données » lorsque les données n'étaient pas collectées auprès de celle-ci mais par d'autres moyens tels que la plaque d'immatriculation d'une voiture[151]. En tout état de cause, en fonction de la sensibilité de certaines bases de données telles celles liées à la lutte contre le terrorisme, le législateur peut prévoir qu'aucune information ne devra être fournie[152]. Cette possibilité s'appliquant de manière générale aux « catégories de traitement » tempère fortement ce droit à l'information additionnelle.

En outre, le titre 2 de la loi du 30 juillet 2018 s'alignant sur la Directive 2016/680, consacre le droit d'accès direct en tant que règle générale et ce, conformément à l'article 8, § 2, de la Charte des droits fondamentaux stipulant que « [t]oute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ». Le responsable du traitement doit donc mettre à disposition de la personne concernée certaines informations telles que : la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées ; les données à caractère personnel en cours de traitement et toute information disponible quant à leur source ; le droit de rectifier ou d'effacer les données, de limiter le traitement des données à caractère personnel ; le droit d'introduire une plainte auprès de l'autorité de contrôle[153].

149 Art. 37, § 1er, 9°, de la loi du 30 juillet 2018.

150 *Doc. parl.*, Ch. repr., sess. ord., 2017-2018, n° 54-3126/001, p. 80. Cette interprétation est conforme au considérant 42 de la Directive 2016/680.

151 C.P.V.P., avis n° 13/2015 du 13 mai 2015 sur l'avant-projet de loi portant dispositions diverses – modifications de la loi portant création d'un organe de recours en matière d'habilitations de sécurité, de la loi sur la fonction de police et de la loi du 18 mars 2014 relative à la gestion de l'information policière (CO-A-2015-019), pt 49.

152 Art. 37, § 3, de la loi du 30 juillet 2018.

153 Art. 38, § 1er, 1° à 8°, de la loi du 30 juillet 2018.

L'accès aux données revêt une importance particulière puisqu'il peut constituer un prérequis pour l'exercice d'autres droits comme le droit à la rectification et le droit à la suppression[154]. En ce sens, la Cour européenne des droits de l'homme a récemment été saisie d'un litige relatif à la conservation de données concernant un militant, M. Catt, dans une base de données policières relatives à « l'extrémisme national ». Pour pouvoir contester la conservation particulièrement longue des données le concernant, M. Catt avait exercé son droit d'accès et obtenu de la police la communication des informations détenues sur son compte. La police lui révéla l'existence dans ses bases de données de soixante-six inscriptions le concernant. Sur la base de ces informations, M. Catt saisit les juridictions internes, arguant notamment que la conservation de ses données n'était pas « nécessaire » au sens de l'article 8, § 2, de la Convention européenne des droits de l'homme. À Strasbourg, la Cour jugea en effet que la conservation prolongée des données dans le cas de M. Catt était disproportionnée dans la mesure où il s'agissait de données à caractère personnel qui révélaient des opinions politiques et méritaient ainsi une protection accrue. De surcroît, M. Catt ne constituait de menace pour personne, compte tenu notamment de son âge. Elle estima par ailleurs que les garanties procédurales n'étaient pas effectives, la durée pendant laquelle les données pouvaient être conservées n'était pas définie, la seule règle à cet égard étant que leur réexamen était prévu au terme d'une période minimum de six ans[155]. Cette affaire met en lumière l'importance du bénéfice d'un droit d'accès direct pour pouvoir former un recours juridictionnel, droit qui n'est par exemple pas prévu pour la Banque nationale générale de données puisque, comme nous le verrons *infra*, la loi sur la fonction de police ne prévoit qu'un accès indirect.

Après avoir exercé son droit d'accès, la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification, éventuellement la complétion ou encore la limitation ou l'effacement des données à caractère personnel la concernant qui sont inexactes[156]. Le responsable du traitement peut, au lieu de procéder à l'effacement, limiter le traitement si l'exactitude des données à caractère personnel est contestée par la personne concernée et qu'il ne peut être déterminé si les données sont exactes ou non, ou si les données à

154 Comité consultatif de la Convention pour la protection des données des personnes à l'égard du traitement automatisé des données à caractère personnel, « Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police », Strasbourg, 15 février 2018, p. 7.

155 Cour E.D.H., *Catt. c. Royaume-Uni*, n° 43514/15, 24 janvier 2019.

156 Art. 39, §§ 1er à 3, de la loi du 30 juillet 2018.

caractère personnel doivent être conservées à des fins probatoires[157]. Le responsable du traitement informe par la suite la personne concernée par écrit des rectifications effectuées ou de tout refus éventuel de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus[158].

En raison des spécificités du domaine pénal, conformément à la Directive 2016/689[159], le titre 2 de la loi du 30 juillet 2018 laisse la possibilité au législateur de retarder ou de restreindre les droits des personnes concernées – le droit à l'information, le droit d'accès, le droit de rectification et à la complétion des données à caractère personnel la concernant qui sont inexactes[160] – par mesures législatives, partiellement ou complètement. Cette restriction doit être nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne concernée, notamment pour les besoins de l'enquête, pour sauvegarder la sécurité publique ou encore pour protéger les droits et libertés d'autrui[161]. En cas de refus éventuel ou de toute limitation éventuelle du droit concerné, le responsable du traitement doit en principe[162] avertir la personne concernée, par écrit, dans les meilleurs délais, des motifs du refus ou de la limitation[163]. Le responsable du traitement doit également informer la personne concernée des possibilités d'introduire une réclamation auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel[164].

De surcroît, le titre 2 stipule également que les droits des personnes concernées s'exercent dans certains cas indirectement, c'est-à-dire par l'intermédiaire de l'autorité de contrôle compétente, dans le respect des principes de nécessité et de proportionnalité dans une société démocratique[165]. Ainsi, pour le traitement de données par les services de police ou l'Inspection générale de la police, le titre 2 de la loi du 30 juillet

157 Art. 39, § 3, de la loi du 30 juillet 2018. Selon le considérant 47 de la Directive 2016/680, les méthodes visant à limiter le traitement de données à caractère personnel pourraient consister, entre autres, à déplacer les données sélectionnées vers un autre système de traitement à des fins archivistiques, ou à rendre les données sélectionnées inaccessibles.

158 Art. 39, § 4, de la loi du 30 juillet 2018.

159 Art. 13, § 3 ; 15, § 1er, de la Directive 2016/680 ; 16, § 4, et consid. 44 de la Directive 2016/680.

160 Art. 38, § 2, et art. 39, § 4, de la loi du 30 juillet 2018.

161 Art. 13, § 3 ; 15, § 1er, de la Directive 2016/680 ; 16, § 4, et consid. 44 de la Directive 2016/680.

162 Pour le droit d'accès, le responsable du traitement n'est pas tenu de fournir cette information si elle crée le risque de compromettre l'un des objectifs visés par cette limitation. Il doit néanmoins consigner les motifs de fait ou de droit sur lesquels se fonde la décision et les mettre à disposition de l'autorité de contrôle compétente (art. 38, §§ 3-4, de la loi du 30 juillet 2018).

163 Art. 37, § 2 ; art. 38, § 3, et art. 39, § 4, de la loi du 30 juillet 2018.

164 Art. 38, § 3, et art. 39, § 4, de la loi du 30 juillet 2018.

165 Art. 41 de la loi du 30 juillet 2018.

2018 prévoit expressément que les droits s'exercent par le biais de l'Organe de contrôle de l'information policière[166]. De même, en cas de traitement par les services de douanes ou par la Cellule de traitement des informations financières, les droits des personnes concernées s'exercent auprès de l'autorité de protection des données[167]. Pour l'Unité d'information des passagers, un accès direct est prévu pour les données fournies par la personne concernée auprès du délégué à la protection des données conformément aux dispositions prévues par le R.G.P.D. et un accès indirect est prévu auprès de l'autorité de protection des données pour les données pour lesquelles l'Unité d'information des passagers a réalisé les contrôles requis[168].

Dans ce cadre, l'autorité de contrôle peut indiquer à la personne concernée qu'elle a « procédé aux vérifications nécessaires » sans pouvoir communiquer si ses droits ont été violés ou non. Elle peut toutefois, dans certains cas, indiquer certaines catégories d'informations contextuelles dans des conditions précisées par le Roi[169]. On peut regretter que cette disposition – qui existait déjà sous l'empire de la loi du 8 décembre 1992[170] – soit restée et reste lettre morte à défaut d'arrêté royal. Or, comme le souligne la Commission de la protection de la vie privée dans son avis, la « transparence par couche » est « indispensable et contribuera à renforcer l'accès au juge, ce qui est un des points de départ poursuivi[s] par le nouveau cadre européen en matière de protection des données à caractère personnel »[171]. Elle rappelle à ce propos que « le nombre de banques de données policières augmente fortement et celles-ci sont consultées ou interrogées pour de nombreuses finalités non policières. Dans des situations spécifiques, les antécédents policiers de citoyens sont même transmis (sous forme abstraite) à des acteurs privés alors que ces acteurs ne font en soi pas partie de la chaîne pénale et de sécurité. Les personnes concernées ne savent par contre généralement pas si (et encore moins pourquoi) leurs données à caractère personnel sont traitées dans une banque de données policière. La réalité sociale nous apprend que la personne dont les données sont enregistrées dans des banques de données policières risque réellement des conséquences

166 Art. 42 de la loi du 30 juillet 2018.
167 Art. 43 de la loi du 30 juillet 2018.
168 Art. 49 de la loi du 30 juillet 2018.
169 Art. 42, al. 4, et art. 43, al. 4, de la loi du 30 juillet 2018.
170 Art. 13, 2, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
171 C.P.V.P., avis 33/2018 relatif à l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 65.

négatives pour sa vie tant professionnelle que privée »[172]. Pour obtenir de telles informations, il revient toutefois préalablement à la personne concernée de communiquer les éléments et circonstances pertinents de la requête afin de pouvoir déterminer si, et si oui, quelles informations peuvent lui être communiquées[173].

Enfin, dans le cadre de poursuites pénales ou d'une procédure judiciaire en matière pénale – que ce soit dans une décision judiciaire, un casier ou un dossier judiciaire –, les droits des personnes concernées s'exercent dans les limites et conformément aux règles et modalités précisées dans le Code judiciaire, le Code d'instruction criminelle, les lois particulières relatives à la procédure pénale et leurs arrêtés d'exécution[174]. Autrement dit, le titre 2 de la loi du 30 juillet 2018 s'applique de manière générale sous réserve des modalités spécifiques prévues par les dispositions légales précitées. À titre illustratif, le Code d'instruction criminelle réglemente le droit d'accès aux données dans le cadre de l'information ou au stade de l'instruction[175].

Section 6. *Prise de décision individuelle automatisée et profilage*

L'article 35 du titre 2 interdit l'adoption de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques « défavorables »[176] ou affectant la personne concernée de « manière significative », à moins d'être assorti de garanties appropriées et d'être autorisé par le droit de l'Union ou par le droit d'un État membre[177]. Les autorités peuvent donc, à l'instar des acteurs privés, procéder à du « *datamining* »[178], technique permettant à l'aide d'al-

172 *Ibid.*
173 *Ibid.*
174 Art. 37, § 4, de la loi du 30 juillet 2018.
175 Art. 21*bis* et 61*ter* du Code d'instruction criminelle. Soulignons qu'auparavant, le Code d'instruction criminelle ne prévoyait pas la possibilité d'introduire un recours devant un juge indépendant et impartial contre la décision du ministère public de refuser l'accès au dossier pénal sur demande du suspect ou d'une partie civile. Un recours a donc été introduit auprès de la Cour constitutionnelle. Celle-ci a considéré que cette absence de recours constituait une atteinte disproportionnée au droit de la défense au sens de l'article 6 de la Convention européenne des droits de l'homme. Un tel argumentaire aurait pu être tenu sur base de l'article 8 de la Convention européenne des droits de l'homme garantissant le droit au respect de la vie privée ou sur la base de l'article 8, § 2, de la Charte garantissant le droit d'accès dans le cadre du droit à la protection des données à caractère personnel (C. const., 25 janvier 2017, n° 006/2017).
176 À la différence du R.G.P.D., la décision ne doit pas uniquement prévoir des effets juridiques, mais ceux-ci doivent être « défavorables » (art. 22, § 1er, du R.G.P.D.).
177 Art. 11 de la Directive 2016/680.
178 À ce propos, voy. L. Orsi, « L'utilisation du big data pour la protection de la sécurité nationale », in *Protection des données personnelles et sécurité nationale*, Bruxelles, Bruylant, 2017, pp. 21 et s.

gorithmes de croiser certaines données et d'anticiper des comportements ou d'établir des profils particuliers.

En cas de décision automatisée, la personne concernée est en droit d'obtenir des informations spécifiques ainsi qu'une intervention humaine lui laissant la possibilité d'exprimer son point de vue et d'obtenir une explication[179]. Afin de garantir l'effectivité des droits de la personne concernée, l'humain doit être en mesure de modifier la décision et d'examiner les données pertinentes, y compris celles fournies par l'intéressé[180]. En ce sens, le système PNR, déjà mentionné *supra*, impose une intervention de l'UIP en cas de concordance positive dans les 24 heures après réception de la notification automatisée de celle-ci[181]. De même, les données collectées suite à l'utilisation de caméras intelligentes de reconnaissance automatique de plaques d'immatriculation sont copiées et conservées à certaines conditions dans la BNG ou les banques de données de bases des services de police[182] après validation manuelle[183].

En raison du risque pour les droits et libertés des personnes concernées, le Groupe 29 recommande aux législateurs nationaux d'imposer au responsable du traitement d'effectuer une analyse d'impact préalable examiné ci-après, et ainsi, d'identifier la nature des garanties spécifiques appropriées devant être adoptées[184].

Section 7. *Principe de sécurité des données*

L'obligation de sécurité imposée au responsable du traitement des données et au sous-traitant se décline en une multitude de sous-obligations relativement similaires à celles contenues dans le R.G.P.D. Cet alignement vise à assurer une certaine cohérence entre les deux textes permettant d'éviter des chevauchements ou confusions susceptibles d'amoindrir le degré de protection des données offert aux personnes

179 Art. 35 de la loi du 30 juillet 2018 ; art. 11, § 1er, et consid. 38 de la Directive 2016/680.
180 Groupe 29, avis 2017, p. 13.
181 Art. 24, § 3, de la loi PNR.
182 En vertu de l'article 44/11/2, § 1er, al. 1er, de la loi sur la fonction de police, « les banques de données de base sont les banques de données policières créées au profit de l'ensemble de la police intégrée et qui ont pour finalité d'exécuter les missions de police administrative et de police judiciaire en exploitant les données à caractère personnel et informations qui y sont incluses et en informant les autorités compétentes de l'exercice de ces missions ».
183 Art. 44/11/3*decies* de la loi sur la fonction de police.
184 Groupe 29, avis 2017, p. 13. En outre, selon le Groupe 29, les lignes directrices adoptées le 3 octobre 2017 sont également pertinentes pour autant que l'on tienne compte des spécificités du domaine pénal. Voy. Groupe 29, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 3 octobre 2017.

concernées[185]. Selon le Groupe 29, ce parallélisme est essentiel compte tenu de l'intensification des échanges entre les autorités répressives et les administrations ou autorités publiques agissant à d'autres fins que celles visées par la Directive 2016/680, mais aussi entre les entités privées et les autorités répressives[186].

En conséquence, le responsable du traitement et le sous-traitant sont tenus d'adopter des mesures techniques et organisationnelles appropriées[187] et, en particulier, de prévoir des règles internes relatives aux principes de « protection des données dès la conception » et de « protection des données par défaut »[188], de tenir un registre des « catégories » d'activités de traitement effectuées sous leur responsabilité[189] (et non des activités de traitement comme le prévoit le R.G.P.D.)[190] et de désigner un délégué à la protection des données[191]. Par ailleurs, en cas de violation de données à caractère personnel, le responsable du traitement doit notifier l'incident à l'autorité de contrôle dans un délai de 72 heures après la prise connaissance, à moins qu'il soit peu probable que la violation en question engendre des risques pour les droits et les libertés d'une personne physique[192]. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard[193]. Comme le précise le Groupe 29, ce délai vise essentiellement à encourager le responsable du traitement à agir rapidement en cas de fuite de données. Compte tenu du fait que le responsable du traitement ne peut toujours être en mesure de notifier une violation de données endéans ce délai, par exemple lorsqu'il subit plusieurs fuites de données sur une courte période ou lorsqu'il décèle au fur et à mesure de nouvelles failles, il peut également notifier à l'autorité de contrôle la violation par phase[194].

185 Groupe 29, avis 03/2015, p. 4.
186 *Ibid.*
187 L'article 50 de la loi du 30 juillet 2018 stipule que « [c]ompte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées. Lorsque cela est proportionné au regard des activités de traitement, ces mesures comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement. Le responsable du traitement est en mesure de démontrer que le traitement est effectué conformément à la loi. Ces mesures sont réexaminées et actualisées si nécessaire ».
188 Art. 51 de la loi du 30 juillet 2018 et art. 25, § 1er, du R.G.P.D.
189 Art. 55 de la loi du 30 juillet 2018.
190 Art. 30 du R.G.P.D.
191 Art. 63 et s. de la loi du 30 juillet 2018 et art. 37 du R.G.P.D.
192 Art. 61, § 1er, de la loi du 30 juillet 2018.
193 Art. 61, § 1er, de la loi du 30 juillet 2018.
194 Groupe 29, Guidelines on Personal data breach notification under Regulation 2016/679, 3 octobre 2017 (version révisée le 6 février 2018), p. 16.

Concernant l'analyse d'impact relative à la protection des données, les dispositions du R.G.P.D. ainsi que les lignes directrices développées par le Groupe 29[195] s'appliquent *mutatis mutandis* pour l'interprétation des dispositions de la Directive 2016/680[196] et, *a fortiori*, à l'article 58 de la loi du 30 juillet 2018. Il incombe donc au responsable du traitement d'effectuer une analyse d'impact des opérations de traitement envisagées lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques compte tenu de la nature, de la portée, du contexte et des finalités du traitement[197]. Cette analyse doit porter sur les systèmes et processus pertinents des opérations de traitement tels des fichiers, et non sur des cas individuels[198]. Elle doit ensuite être fournie à l'autorité de contrôle, sur demande ou dans le cadre d'une consultation préalable, afin de lui permettre d'apprécier la conformité du traitement et les risques pour les droits et liberté des personnes physiques[199].

Par ailleurs, lorsque le traitement des données à caractère personnel implique la création d'un nouveau fichier, le responsable du traitement ou le sous-traitant doit consulter préalablement l'autorité de contrôle dans deux situations. En premier lieu, si l'analyse d'impact indique que le traitement pourrait présenter un risque élevé dans le cas où le responsable du traitement ne prendrait pas de mesures pour atténuer le risque. En second lieu, si le type de traitement, en particulier compte tenu de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées[200]. Si l'autorité de contrôle estime que le traitement pourrait entraîner une violation des dispositions adoptées en vertu du titre 2 de la loi du 30 juillet 2018, elle fournit un avis écrit et non contraignant dans un délai maximum de six semaines à compter de la réception de la demande de consultation, contenant le cas échéant des mesures correctrices dans les conditions prévues par la loi et telles que détaillées

195 Groupe 29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, 4 avril 2017.

196 Groupe 29, avis 01/2013 apportant une contribution supplémentaire aux discussions sur la proposition de directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale p. 6 ; Commission de la protection de la vie privée, Recommandation n° 01/2018 concernant l'analyse d'impact relative à la protection des données et la consultation préalable, 28 février 2018.

197 Art. 58, § 1er, de la loi du 30 juillet 2018 ; art. 27, § 1er, de la Directive 2016/680 et art. 35, § 1er, du R.G.P.D.

198 Consid. 58 de la Directive 2016/680.

199 Art. 59, § 3, de la loi du 30 juillet 2018.

200 Art. 59, § 1er, de la loi du 30 juillet 2018.

infra[201]. L'autorité de contrôle doit également être consultée dans le cadre de l'élaboration d'une proposition de mesure législative ou d'une mesure réglementaire fondée sur cette base[202], mais aussi en vertu d'une liste des opérations de traitement qu'elle peut établir[203]. En outre, l'article 60, § 2, du titre 2 prévoit une série de mesures à mettre en œuvre par le responsable du traitement ou le sous-traitant, en cas de traitement automatisé, à la suite d'une évaluation des risques[204].

Remarque importante, à la différence du R.G.P.D., le titre 2 de la loi du 30 juillet 2018 impose expressément la tenue de journaux ou de « *logs* » dans le cadre de différentes opérations de traitement telles la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement de données[205]. Ces journaux doivent indiquer : le motif, la date et l'heure de l'opération ; les catégories de personnes ou, dans la mesure du possible, l'identification de la personne qui a consulté les données ; les systèmes qui ont communiqué ces données ; et les catégories de destinataires des données à caractère personnel et, si possible, l'identité des destinataires de ces données[206]. Ils doivent être mis à disposition de l'autorité de contrôle, sur demande[207], afin qu'elle puisse vérifier la licéité de certaines opérations, d'effectuer des autocontrôles, en ce compris dans le cadre de procédures disciplinaires internes des autorités compétentes[208]. Ils permettent également de garantir l'intégrité et la sécurité des données dans

201 Art. 59, § 4, de la loi du 30 juillet 2018.
202 Art. 59, § 1er, de la loi du 30 juillet 2018.
203 Art. 59, § 2, de la loi du 30 juillet 2018.
204 Ces mesures sont destinées à (a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations) ; (b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données) ; (c) empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation) ; (d) empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs) ; (e) garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données) ; (f) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission) ; (g) garantir qu'il puisse être vérifié et constaté *a posteriori* quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction) ; (h) empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport) ; (i) garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration) ; (j) garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).
205 Art. 56, § 1er, al. 3, de la loi du 30 juillet 2018.
206 Art. 56, § 1er, al. 2, de la loi du 30 juillet 2018.
207 Art. 56, § 3, de la loi du 30 juillet 2018.
208 Art. 56, § 1er, al. 3, de la loi du 30 juillet 2018.

le cadre de procédures pénales[209], par exemple lorsque la légalité d'une opération de traitement de données est contestée ou lorsqu'une violation de données à caractère personnel est en jeu[210].

Comme le souligne le Groupe 29, l'implémentation des *logs* est un outil crucial en protection des données puisqu'il permet de contrôler les opérations effectuées, de retracer l'activité des utilisateurs et de détecter les utilisations abusives recouvrant dès lors, à la fois, un aspect dissuasif et un aspect sanctionnateur[211]. En ce sens, l'article 44/11/12, § 2, e), 2°, de la loi sur la fonction de police impose l'enregistrement des « *logs* » relatifs aux accès à la B.N.G. de toutes les transactions et la conservation de ces données pendant dix ans minimum[212]. Cette journalisation s'exerce tant à des fins de contrôle préventif qu'à des fins opérationnelles pour, notamment, vérifier si une personne ou un moyen de transport a été contrôlé par un service de police[213]. Notons toutefois qu'en dépit de ces garanties, un rapport du Comité P met en évidence l'importance des consultations illégitimes de banques de données mises à disposition des services de police et ceci, en particulier, en dehors du cadre professionnel, généralement pour des motifs d'ordre privé comme la curiosité[214]. Il préconise dès lors, outre l'enregistrement des accès, l'enregistrement du motif de la consultation, afin de freiner les consultations abusives[215].

Section 8. *L'autorité de contrôle indépendante*

Comme l'a rappelé la Cour de justice de l'Union européenne à l'occasion de l'arrêt *Schrems*, l'institution d'une autorité de contrôle indépendante constitue un élément essentiel du respect de la protection des données[216]. Dans la même lignée, l'importance de l'Organe de contrôle de l'information policière (ci-après C.O.C.) et de ses missions a été récemment soulignée par la Cour constitutionnelle à l'occasion d'un

209 Art. 56, § 3, de la loi du 30 juillet 2018.
210 Groupe 29, avis 2017, p. 27.
211 Groupe 29, avis 2017, p. 26.
212 Cette disposition a été insérée par l'article 35 de la loi du 18 mars 2014, relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle, *M.B.*, 28 mars 2014.
213 *Doc. parl.*, Ch. repr., sess. ord., 2013-2014, n° 53-3105/001, p. 35.
214 Comité P, *Rapport établi dans le cadre de l'enquête de contrôle relative aux accès illégitimes aux banques de données par les membres des services de police*, Dossier n° 21530/2015. Voy. égal. le Comité P, rapport annuel 2017, p. 108, disponible sur le site internet du Comité P (http://www.comitep.be).
215 Comité P, *op. cit.*, p. 28.
216 C.J.U.E., 6 octobre 2015, *Schrems c. Data Protection Commissionner of Ireland*, C-362/14, § 41.

recours relatif à la loi sur la gestion de l'information policière[217]. La cour évacua tout doute d'inconstitutionnalité relatifs aux différents points soulevés par les requérants tels que le traitement de données sensibles, le transfert international des données, les délais de conservation des données en faisant référence au C.O.C., l'érigeant en véritable gardien de la protection des données.

Précisons à toutes fins utiles que la Directive 2016/680 laisse le soin aux États membres d'opter pour une autorité de contrôle indépendante spécifique ou compétente à la fois pour contrôler les opérations effectuées sous le volet du R.G.P.D. et de la Directive[218]. En l'occurrence, l'Organe de contrôle de l'information policière agit comme autorité de protection des données pour les services de la police, l'Inspection générale de la police fédérale et locale ainsi que pour l'Unité d'information des passagers[219]. En revanche, la loi n'indique pas quelle est l'autorité de contrôle des autres autorités compétentes, à savoir le Service d'enquêtes du Comité R et du Comité P, l'Administration générale des douanes et accises et la Cellule de traitement des informations financières. Elles devraient donc être soumises au contrôle de l'Autorité de la protection des données, sauf si une loi prévoit un régime dérogatoire[220]. Par contre, l'Autorité de protection des données n'est pas compétente pour contrôler les traitements effectués par les cours et tribunaux ainsi que le ministère public dans l'exercice de leur fonction juridictionnelle[221] pour lesquels, comme nous le verrons ci-après, le C.O.C. est compétent.

Le C.O.C. est chargé de surveiller l'application des dispositions contenues dans le titre 2[222], de veiller à la légalité du contenu de la Banque de données nationale générale, les banques de données de base, les banques de données particulières et les banques de données techniques, ainsi que la procédure de traitement des données et informations qui y sont conservées[223] ou encore d'émettre des avis, d'initiative ou sur demande sur toute question relative à la gestion de l'information policière[224]. Pour mener à bien ses missions, il dispose d'un service d'en-

217 C. const., n° 108/2016, 14 juillet 2016, consid. B.22, B.26.2, B.49, B.67.4, B.85, B.91, B.92, B.97, B.98.4.3, B.99.3.3, B.99.3.4, B.107.3, B.112.6, B.115.9, B.113.2, B.124.2, B.133 et B.155.

218 Art. 41, § 3, de la Directive 2016/680.

219 Il s'agit des autorités visées à l'art. 26, 7°, a), d), et f), de la loi du 30 juillet 2018.

220 Art. 4, § 2, al. 2, de la loi du 30 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018 et *Doc. parl.*, Ch. repr., sess. ord., 2017-2018, n° 54-3126/001, p. 408.

221 Art. 4, § 2, al. 1er, de la loi du 30 décembre 2017 portant création de l'Autorité de protection des données.

222 Art. 71, § 1er, de la loi du 30 juillet 2018.

223 Art. 239, § 1er, de la loi du 30 juillet 2018.

224 Art. 236, § 1er, de la loi du 30 juillet 2018.

quête pouvant procéder à l'audition de personnes[225], accéder de manière illimitée aux informations et aux données traitées par les services soumis à leur contrôle mais aussi aux locaux où se trouvent ces données[226]. Au besoin, ce service peut requérir l'assistance de la force publique et effectuer les constatations qui s'imposent[227], mais aussi saisir dans ces lieux tous les objets, documents et données d'un système informatique utiles pour leur enquête, à l'exception de ceux qui concernent une information ou une instruction judiciaire en cours[228].

Notons que tous les services de l'État, y compris les parquets et les greffes des cours et tribunaux, sont tenus, vis-à-vis du C.O.C., de ses membres ou des membres du service d'enquête et à leur demande, de leur fournir tous les renseignements que ces derniers estiment utiles au contrôle du respect de la législation dont ils sont chargés, ainsi que de leur produire, pour en prendre connaissance, tous les supports d'information et de leur en fournir des copies sous n'importe quelle forme[229]. Toutefois, si ces renseignements font partie d'une enquête pénale ou judiciaire en cours, ils ne seront transmis que moyennant l'autorisation préalable du ministère public compétent[230]. Cette interprétation paraît conforme à la Directive 2016/680 puisqu'en principe, l'autorité de contrôle désignée, à savoir le C.O.C., n'est pas compétente pour contrôler les opérations de traitement effectuées, d'une part, par les juridictions[231] dans l'exercice de leur fonction juridictionnelle « afin de préserver l'indépendance des juges dans l'accomplissement de leurs missions judiciaires » et, d'autre part, par le ministère public[232].

Enfin, le C.O.C. est l'instance compétente pour assurer le suivi des réclamations et plaintes et est tenu d'informer l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire[233]. Il a le pouvoir de rappeler à l'ordre les différentes autorités compétentes soumises à son contrôle en cas de violation d'une disposition de la réglementation relative aux traitements des données à caractère personnel[234], mais aussi

225 Art. 245, § 1er, de la loi du 30 juillet 2018.
226 Art. 244, § 1er, de la loi du 30 juillet 2018.
227 Art. 244, § 3, de la loi du 30 juillet 2018.
228 Art. 244, § 2, de la loi du 30 juillet 2018.
229 Art. 246, al. 1er, de la loi du 30 juillet 2018.
230 Art. 246, al. 2, de la loi du 30 juillet 2018.
231 Art. 45, § 2, de la Directive 2016/680.
232 Consid. 80 de la Directive 2016/680.
233 Art. 240, al. 1er, 4°, et 247 de la loi du 30 juillet 2018.
234 Art. 247, al. 3, de la loi du 30 juillet 2018.

d'ordonner de mettre un traitement en conformité avec la réglementation applicable[235], ou encore d'interdire temporairement ou définitivement un traitement de données[236].

Section 9. *Transferts internationaux de données*

Le titre 2 autorise les transferts internationaux de données par les autorités compétentes vers un pays tiers ou à une organisation internationale qualifiée d'autorité compétente[237], à des fins pénales[238], sous réserve de l'adoption d'une décision d'adéquation adoptée par la Commission, ou en l'absence d'une telle décision, de garanties appropriées ou, en l'absence de garanties appropriées, dans le cadre des dérogations pour des situations particulières[239]. Revenons brièvement sur ce régime en cascade.

En l'absence de décision d'adéquation, le responsable du traitement peut autoriser le transfert de données vers un pays tiers ou à une organisation internationale sous réserve de l'existence de garanties appropriées en matière de protection des données directement évaluées par ce dernier ou édictées dans un instrument juridique contraignant[240]. Le C.E.P.D. recommandait néanmoins de limiter le transfert de données aux situations où il existe un instrument juridiquement contraignant, ou lorsqu'il est nécessaire de protéger les intérêts vitaux de la personne concernée ou dans le cas d'une menace grave et immédiate à la sécurité publique[241] et ce, conformément aux conditions exposées dans la recommandation R (87)15. En tout état de cause, ces transferts devraient être documentés et mis à la disposition de l'autorité de contrôle, sur demande, afin qu'elle puisse en vérifier la licéité[242].

Notons que, selon l'article 61 de la Directive 2016/680, les accords applicables avant l'entrée en vigueur de la Directive demeurent inchangés. En effet, dans la mesure où antérieurement, les transferts de données entre l'UE et les pays tiers dans un contexte répressif n'étaient pas subordonnés à l'existence d'une décision d'adéquation, des accords bilatéraux ont été conclus entre l'UE et des pays tiers. À titre illustratif,

235 Art. 247, al. 4, de la loi du 30 juillet 2018.
236 Art. 247, al. 5, de la loi du 30 juillet 2018.
237 Art. 66, § 1er, b, de la loi du 30 juillet 2018.
238 Art. 27 et 66, § 1er, a, de la loi du 30 juillet 2018.
239 Art. 66, § 1er, d, de la loi du 30 juillet 2018.
240 Art. 68, § 1er, de la loi du 30 juillet 2018.
241 C.E.P.D., avis n° 6/2015, p. 9.
242 Art. 68, § 3, de la loi du 30 juillet 2018.

l'accord-cadre sur la protection des données signé entre les États-Unis et l'UE[243] est, selon la Commission européenne, particulièrement complet et pourrait servir de base pour négocier des décisions d'adéquations futures avec des pays tiers non seulement dans le domaine de la coopération judiciaire et policière, mais aussi dans d'autres domaines de l'application de la loi par les autorités publiques (par exemple la politique de concurrence ou la protection des consommateurs)[244].

En l'absence de garanties appropriées constatées par le responsable du traitement, un transfert de données vers un pays tiers ou à une organisation internationale est autorisé dans un nombre limité de situations, à savoir si ce transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ; à la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ; dans un cas particulier, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; ou, dans un cas particulier, à la constatation, l'exercice ou la défense de droits en justice[245]. À ce propos, le considérant 72 de la Directive 2016/680 précise que « ces dérogations devraient être interprétées de manière restrictive et ne devraient pas permettre des transferts fréquents, massifs et structurels de données à caractère personnel ni des transferts de données à grande échelle, mais des transferts qui devraient être limités aux données strictement nécessaires ».

De plus, lorsque des données proviennent d'un autre État membre et sont transférées ultérieurement vers un autre pays tiers ou à une autre organisation internationale, l'État membre ayant traité les données initialement doit en règle générale donner son consentement avant le transfert conformément à son droit national[246]. À cette fin, ce dernier est tenu de prendre en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction pénale, la finalité pour laquelle les données à caractère personnel ont été transférées initialement et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel/laquelle les données

243 Accord, entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, *J.O.*, L 336, 10 décembre 2016, pp. 3 et s.

244 *Communication* de la Commission au Parlement et au Conseil, « Échange et protection de données à caractère personnel à l'ère de la mondialisation », COM (2017) 7, 10 janvier 2017, p. 16.

245 Art. 69, § 1er, de la loi du 30 juillet 2018.

246 Art. 66, § 1er, 5°, de la loi du 30 juillet 2018.

à caractère personnel sont transférées ultérieurement[247]. Par exception, une autorisation ne doit pas être requise dans la situation où ce transfert est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre et si l'autorisation préalable ne peut pas être obtenue en temps utile[248]. L'État membre ayant traité les données initialement doit cependant en être informé sans retard[249].

En outre, si en principe la coopération policière et judiciaire s'exerce entre les autorités compétentes, le droit de l'Union ou le droit d'un État membre peut dans certains cas particuliers autoriser le transfert de données à caractère personnel vers d'autres types de destinataires établis dans des pays tiers[250]. Cette situation pourrait se présenter en cas d'attentat terroriste imminent où l'autorité compétente cherche à obtenir en urgence l'identité du titulaire d'un compte bancaire auprès d'une banque située hors du territoire de l'Union européenne. À cette fin, le titre 2 transposant la Directive 2016/680 impose le respect des critères de nécessité, proportionnalité et subsidiarité[251]. Ensuite, l'autorité compétente dans le pays concerné doit être informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié. De plus, l'autorité compétente effectuant le transfert informe également le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel ne doivent faire l'objet d'un traitement que par cette dernière, à condition qu'un tel traitement soit nécessaire[252]. En outre, l'autorité compétente qui transfère les données informe l'autorité de contrôle des transferts et documente ce transfert[253].

247 Art. 66, § 1er, 5°, de la loi du 30 juillet 2018.
248 Art. 66, § 2, de la loi du 30 juillet 2018.
249 *Ibid.*
250 Art. 70, § 1er, de la loi du 30 juillet 2018.
251 Plus précisément, la disposition impose de s'assurer que le transfert est strictement nécessaire à l'exécution de la mission de l'autorité compétente qui transfère les données ; l'autorité compétente qui transfère les données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas en question ; l'autorité compétente qui transfère les données estime que le transfert à une autorité qui est compétente, dans le pays tiers est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun et informe dans les meilleurs délais cette dernière de ce transfert.
252 Art. 70, § 1er, de la loi du 30 juillet 2018.
253 Art. 70, §§ 2-3, de la loi du 30 juillet 2018.

Conclusion

Malgré des différences importantes au sein des systèmes judiciaires des États membres, la Directive 2016/680 se donne pour objectif ambitieux de légiférer dans le domaine de la « police » et de la « justice », domaine traditionnellement considéré comme relevant de leur souveraineté nationale. Alors que la décision-cadre 2008/977 limitait son champ d'application aux flux transfrontières de données, la Directive 2016/680 s'applique aux traitements de données effectués sur le territoire interne des États membres et au-delà. Plus qu'un cadre visant à favoriser l'échange de données à des fins de coopération policière et judiciaire, elle offre une base commune de protection des données dans un contexte répressif tout en cherchant à ménager un équilibre entre le besoin de garantir la sécurité publique et la nécessité de protéger le droit à la protection des données à caractère personnel.

Le titre 2 de la loi du 30 juillet 2018 transpose fidèlement la Directive 2016/680 sous réserve du champ d'application limité en raison de l'énumération par le législateur des différentes « autorités compétentes ». Toutefois, comme déjà souligné, cela n'apparaît pas problématique à première vue puisque la personne concernée devrait dès lors bénéficier des droits et garanties conférés par le R.G.P.D., droits *a priori* plus étendus que ne le prévoit la Directive 2016/680.

Néanmoins, il est regrettable que les droits des personnes concernées n'aient pas été davantage affirmés et soient amputés d'exceptions. En ce sens, le titre 2 de la loi du 30 juillet 2018 prévoit un droit à l'information tout en laissant la possibilité au législateur de prévoir des « catégories de traitement » pour lesquelles aucune information ne devra être fournie[254]. De même, le droit d'accès direct est généralisé tout en organisant un panel important d'exceptions permettant de limiter, partiellement ou totalement, ce droit pour diverses raisons telles que les nécessités de l'enquête. De surcroît, en cas d'accès indirect même si le législateur prévoit que pour certaines catégories de traitement des informations contextuelles peuvent être fournies à la personne concernée, cela suppose l'adoption d'un arrêté royal qui, même par le passé, n'a jamais été adopté. Ces exceptions au droit à l'information et au droit d'accès sont particulièrement regrettables puisque ceux-ci peuvent s'avérer essentiels pour permettre aux personnes concernées d'exercer d'autres droits tels que la

[254] Art. 37, § 3, de la loi du 30 juillet 2018.

rectification ou la suppression des données concernées, comme l'illustre l'arrêt *Catt c. Royaume-Uni* récemment rendu par la Cour européenne des droits de l'homme[255].

Même si l'on peut s'interroger sur les réelles incidences de la loi du 30 juillet 2018 compte tenu des nombreuses possibilités d'y déroger *via* l'adoption de lois « sectorielles », saluons la cohérence de la Directive 2016/680 et du titre 2 de la loi du 30 juillet 2018 vis-à-vis du R.G.P.D. au niveau des règles relatives à la protection des données et compte tenu de l'intensification des échanges entre les entités privées et les autorités répressives, voire du rôle de plus en plus étendu que les autorités répressives leur accorde dans la collecte de preuves. Toutefois, une faiblesse majeure inhérente à l'adoption d'un instrument spécifique dans le domaine de la protection des données est celle d'aboutir à une restriction des garanties offertes aux personnes concernées en raison des besoins de la « police » et de la « justice ».

Février 2019

255 Cour E.D.H., *Catt. c. Royaume-Uni*, n° 43514/15, 24 janvier 2019.